Policy and Guidelines on the Use of the Internet

Lead Directorate and Service:	Corporate Resources / Human Resources
Effective Date:	October 2016
Contact Officer/Number:	HR Advice Centre/391221
Approved by:	The Cabinet 17.7.07 Min: 3020/ CMT 1.3.10 Min: 12308, DR 10783: 16.3.10/ CMT 11.2.13 Min: 14839, DR 14271: 20.3.13/ CMT 2.8.16 Min: 17081, The Cabinet 18.10.16/Min: 5584

Policy on the Use of the Internet

1. Scope

1.1 This Policy and Guidelines apply to all employees of the Council including school based employees where it has been adopted by the respective school governing body and any third party carrying out work on behalf of the Council or accessing the Council's information systems. Within schools this policy applies to all administrative access via the corporate network, ie Central Simms, internet and e-mail. School curriculum access is provided separately and not supported by the corporate network, schools should therefore refer to their own policies covering school curriculum access as this policy does not apply to curriculum access.

1.2 This Policy is produced for the guidance of employees accessing data published by other organisations and available on the Internet. Employees wishing to publish Council data on the World Wide Web must do so in accordance with the Council's separate guidelines and procedures on the publication of data via the Internet. All Council information published on the Council's web-site, www.eastriding.gov.uk is managed by individual service managers and is monitored by the Council's Communications Team with strategic oversight by the Customer Strategy and Digital Service Team.

2. Background

2.1 East Riding of Yorkshire Council promotes the use of the Internet by its citizens and staff, as a primary vehicle for the dissemination, publication and gathering of information. The Council encourages the responsible use of the Internet by its employees.

2.2 Internet facilities are provided by the Council as a business tool to enable its employees to enhance the efficiency and effectiveness of their work for the Council.

3. Definitions for the Purpose of this Policy

3.1 The term Internet refers to the worldwide, publicly accessible network of interconnected computer networks that transmit data by packet switching using the standard Internet Protocol (IP).

3.2 The term streaming media refers to multimedia that is continuously received by, and normally displayed to, the end-user. Streaming media technologies include, but are not limited to; webcasts, video, voice over IP, videoconferencing, web TV, Internet radio.

3.3 The term 'social media' is commonly given to websites and online tools which allow users to interact with each other in some way - by sharing information, opinions, knowledge and interests. Social media can be referenced in a variety of ways, examples of these are, but not limited to: Blogs, Facebook, Collaborative spaces (eg Wetpaint), Media sharing services (eg YouTube) 'Microblogging' applications (eg Twitter, Linked In).

4. Policy Statement

4.1 This Policy and Guidelines on the use of the Internet has been produced to ensure that Council employees are fully aware of the rules concerning the use of the Internet and the actions that could result should any misuse be detected.

5. Responsibility

5.1 All Directors, senior managers and delegated managers will be responsible for ensuring that the policy is applied consistently within their Directorate. As part of the induction process an employee must be made fully aware of the policy. The employee's manager must discuss the policy with the employee to ensure the employee understands its content.

5.2 An employee is responsible for reading the Policy and Guidelines on the Use of the Internet at the start of their employment and should ensure any concerns or queries are raised with their manager prior to accessing the internet.

6. Policy Review

6.1 This Policy will be reviewed in line with the Council's rolling policy review programme by Human Resources and the Corporate ICT Section in consultation with relevant departments and recognised Trade Unions.

7. Links to Other Policies/References

Disciplinary Policy and Procedure
IT Security Policy
IT Security Incident Response Procedures
Data Protection Policy
Policy and Guidelines on the Use of Electronic Mail (Email)
Social Media Guidelines
Equality Legislation
ICT Computer Usage Policy
Mobile Device Policy and Procedure

Guidelines on the Use of the Internet

1. Introduction

1.1 The Internet is a series of communication links which enables computers around the world to access information and exchange files. The Internet allows users to obtain information held (and published) on computers anywhere in the world easily and relatively quickly. It also allows users to send information (such as orders) back to these computers. It is a huge free-standing network to which millions of users have access.

1.2 The legitimate business use of the Internet has increased beyond expectations in the last few years and all the indications are that this increase will continue. Many organisations now make essential information available only via the Internet and many Council Directorates are dependent upon Internet access for up-to-date and business critical information.

1.3 The open design of the Internet is its strength. However, the lack of controls and standards also exposes organisations (and private individuals) to an increased risk that networks and systems will be accessed improperly, data corrupted and viruses introduced. The Internet does not guarantee the privacy and confidentiality of information. Any material transferred over the Internet may be at risk of detection by a third party. Employees must exercise caution and care when transferring such material in any form.

2. Internet Gateway

2.1 The Internet Gateway via the corporate network will be managed, maintained and monitored by IT Services on behalf of the Council including when provided and used within schools.

2.2 All connections to the Internet will be made via the Internet Gateway using the corporate network. Where this is provided within schools this will include all administration access which is simply an extension of the corporate network, eg Access to central Simms, internet, email etc. Exceptions will be where Internet access is needed either at a site which is not on the corporate network, or on a portable computer or other mobile devices for either remote working or Internet demonstration purposes.

2.3 All workstations must use the corporate proxy servers and must auto detect proxy settings. Specific exceptions on technical grounds may be permitted subject to the approval of the Corporate ICT Manager. Use of external or anonymous proxy servers is specifically forbidden.

2.4 All Internet users must authenticate using a network username and password when accessing Internet sites. These passwords must remain confidential and should not be divulged to any other person. Some business related sites may bypass this authentication where continuous connections are required.

2.5 The connection of personal ipods/MP3 players/digital cameras or mobile phones to Council computing devices is prohibited unless specific authority has been given by the Corporate ICT Manager. Please also refer to the ICT Computer Usage Policy.

2.6 The Council will routinely monitor Internet usage and will maintain logs of Internet activity as means of ensuring compliance with this Policy.

3. Authorised Internet Users

3.1 The Council wishes to encourage its employees to use the Internet and as such will provide Internet access to staff connected to the corporate network. The primary purpose of Internet access must be for business use. Limited personal use is permitted in an employee's non working time subject to the guidance at section 5, but may be withdrawn at times of high business demand. Employees with Internet access are also encouraged to use the facility for their own personal development and training in agreement with their line manager.

3.2 Employees authorised to access the Internet must ensure, whenever practically possible, that the facility is not used by employees who have not been given access or by anyone who is not an employee of the Council. An employee with Internet access must not allow another member of staff access to the Internet via their password.

3.3 Employees, irrespective of whether or not they themselves are authorised Internet users, are required to inform an appropriate manager if they become aware of, or suspect, the Council's Internet facilities are being misused.

4. Unacceptable Use

4.1 It is illegal to create, access, copy, store, transmit or publish any material which falls into the following categories:

a) National Security: instructions on bomb-making, illegal drug production, terrorist activities.

b) Protection of Minors: inappropriate forms of marketing, displays of violence or pornography involving minors.

c) Protection of Human Dignity: incitement to racial hatred or racial discrimination, harassment.

d) Economic Security: fraud: instructions on pirating credit cards.

e) Information Security: malicious hacking.

f) Protection of Privacy: unauthorised communication of personal data, electronic harassment.

g) Protection of Reputation: libel: unlawful comparative advertising.

h) Intellectual Property: unauthorised distribution of copyrighted works, eg software or music.

4.2 It is unacceptable to create, access, copy, store, transmit or publish any material which:

a) Is obscene or pornographic as defined by the Internet Watch Foundation.

b) Is likely to irritate or waste time of others.

c) Is subversive to the purposes of the Council.

d) Is likely to corrupt others.

For the purposes of these Guidelines, obscene and pornographic are defined as follows:

Obscene - indecent, lewd, repulsive.
Pornographic - perverted, indecent.

When assessing whether material is unacceptable, each case will be judged on its merits, taking into account the individual circumstances.

4.3 It is prohibited to undertake any activity which is intended to:

a) Corrupt any information held or transmitted on the Internet.

b) Detect weaknesses in any security infrastructure (testing firewalls, cracking passwords).

c) Disrupt the normal functioning of the Internet or related services (overloading transactions, introducing viruses, denial of service).

4.4 No executable software may be downloaded from the Internet other than by authorised IT Services staff, who can be contacted via the IT Service Desk on extension 4444.

4.5 The playing of games via the Internet is not permitted.

4.6 Access to non-work related on-demand or live streaming media is prohibited. Streaming media technologies include, but are not limited to; chat rooms, webcasts, video, voice over IP, videoconferencing, web TV, Internet radio. Websites that stream media content include, but are not limited to; youtube, myspace, google videos, skype, facebook, flickr, dimdim, twitter.

4.7 Access to social media during work time for personal use is not permitted**.** Employees are only permitted to use social media for work purposes (professional use) with the express prior permission of their Head of Service and Director that the use of social media will form part of an employee's role and the manager must agree in advance the scope context and timings of its use, otherwise all access to social media through the Council IT system is not permitted. Employees who are able to use social media must adhere to applicable Council policies. Council employees are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media.

5. Personal Use

5.1 The Council's Internet facilities may be used within permitted periods for personal use.

5.2 The Internet facilities must not be used in pursuance of any business (profit making or otherwise) other than that of the Council. Similarly, organising clubs or societies using the Council's Internet links is also not allowed.

5.3 The internet facilities must not be used to access social media for personal use from a council computer either at work or at home.

5.4 Any personal use must be undertaken in accordance with the following criteria:-

a) Access to the Internet must only be made in the employee's own non working time ie. before or after their working start and finish time or in their lunch break. An employee's work pattern as entered onto i-Trent will be the definitive record for defining an employees work/non work pattern.

b) The following limitations on use apply to all staff:

- No personal access during working hours is allowed.
- Legitimate information (that does not fall under section 4 - Unacceptable Use) searched for and found on the Internet may be printed provided the volumes are reasonable (eg 2 or 3 pages only) and the information to be printed satisfies the rules for personal use.
- Personal use must be kept to a reasonable level, and may be monitored to ensure compliance.
- Access during an individual's lunch break is allowed but is limited to a maximum of 30 minutes.

5.5 Purchasing personal goods and services over the Internet is permitted. Staff must not follow links to e-commerce websites, the address must be typed every time to avoid fraudulent sites. Browser caches and history should be cleared after each session where financial transactions are carried out. Staff must not enter any work related details when purchasing personal goods or services, including using a Council email account as a method of contact. The Council will accept no liability for purchases made using the Council's Internet facilities and staff should not have goods delivered to their work address.

5.6 Purchasing Council goods and services over the Internet is permitted but staff are reminded that the Council's preferred method of procurement is via the P2P procurement system. However some goods and services, for example Internet domain names, are only available via the Internet and staff must ensure that for Council purchases via the Internet a Council issued purchase card must be used and the sites being procured from must be using secure protocols. This is normally indicated with a visible padlock in the browser.

5.7 The business use of the Council's IT facilities overrides all personal use at all times. Personal use may be withdrawn at short notice if traffic levels impact on business use. A global email will be sent informing staff of any such withdrawals.

8 Staff working on PCs in front-line locations must not access the Internet in view of the public for personal reasons at any time, regardless of whether their personal working pattern has yet to start or has been completed.

6. Incident Management and Monitoring

6.1 IT Services has defined a security incident response procedure. Employees must contact the IT Service Desk if they are aware of, or suspect, a breach of the Internet Use Policy. The IT Security Incident Response Procedure is available on the Intranet.

6.2 The Council will monitor the use of the Internet by staff and reserves the right to inspect all files stored on network servers; PCs, laptops and mobile devices to ensure compliance with the Policy.

7. Misuse

7.1 Any identified misuse of the Internet facilities will be investigated and could result in action under the Council's disciplinary policy and procedure.

7.2 Examples of misuse could include excessive personal or inappropriate use of the Internet, personal use during normal working hours, downloading executable files or accessing non-work related streaming media. The above list is not exhaustive.