Internet Use Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Risks
  - Policy Details
  - Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Internet Use Policy

Background

Canterbury City Council, Dover District Council, and Thanet District Council (The Councils) provide technology devices, such as PCs, laptops, thin client devices, Blackberrys, iPads, iPhones and other smart devices, together with access to the Internet. This policy will ensure all users of the councils provided internet facilities are aware of the acceptable use of such facilities.

There are a number of legislative requirements that must be adhered to in relation to telephony, IT networks and any specific applications, e-mail and Internet use. The acceptable use policy defines for all users what is acceptable and unacceptable use of council systems and equipment.

This Internet Acceptable Usage Policy should be applied at all times whenever using the councils provided Internet facility. This includes access via any access device including a desktop computer, laptop computer or mobile device. Users are also reminded that comments made on social networking sites, chat rooms etc. are in the public domain and must not bring the councils or their partners into disrepute, or be of a defamatory nature. The councils will not tolerate bullying or harassment of colleagues in any form, this includes via social networking.

This policy outlines your personal responsibilities and informs what you must and must not do.

The Internet facility is made available for the business purposes of the councils. A certain amount of such use must not interfere with is permitted in accordance with the statements contained within this Policy.

Key Messages

- Users must familiarise themselves with the detail, and spirit of this policy before using the Internet.

- Users are responsible for ensuring the security of their account logon-id and password. Individual user log-on id and passwords should only be used by that individual user, and they should be the only person who accesses their Internet account.

- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other material that might be deemed illegal, obscene or offensive.

- Users must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism for the task.

- At the discretion of your line manager and provided it does not interfere with your work, the councils permit some personal use of the Internet in your own time (for example during your lunch-break).

Risks

The councils recognise that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The introduction of viruses and malware on to the councils' ICT network.

- The downloading and/or display of inappropriate or offensive material.

- Information and data security incidents.

- The downloading of unauthorised software.

- Damage to the reputation of The Councils.

Non-compliance with this policy could have a significant effect on the efficient operation of The Councils and may result in financial loss, legal action and/ or an inability to provide necessary services to our customers.

Policy Detail

Remote Use

Users will sometimes need to use council equipment and access the council network when working remotely, whether from their home, offsite or when travelling. Remote users are reminded that this policy applies to them wherever they are using council owned equipment and/or accessing the council network from a non-council device.

Before using or taking council equipment overseas you must seek advice from ICT Services

Personal Use of the Council's Internet Service

At the discretion of your line manager and provided it does not interfere with your work, the councils permit reasonable personal use of the Internet in your own time (for example during your lunch-break or after work) provided this is strictly in accordance with the terms of this policy.

If you are in any doubt about how you may make personal use of the councils' Internet Service you are advised not to do so without first seeking the advice and approval of your line manager.

Such use must not interfere with your council work or the work of the councils. The councils reserve the right to withdraw this privilege if they consider that it is being abused. If excessive personal use is suspected and subsequently proved then managers would be permitted to prevent all personal use and consider disciplinary action.

Personal use of the internet may be withdrawn for operational reasons.

You must be aware that the security systems cannot distinguish between personal and official use of the Internet. Your web access will be subject to the same monitoring processes, and may be revealed to ICT, Audit and your own management or other authorised parties.

You must not use the Internet facilities for any other business or commercial purpose.

Internet Account Management, Security and Monitoring

The councils will provide a secure logon-id and password facility for your network account. EK Services ICT department is responsible for the technical management of this account. You are responsible for the security provided by your account logon-id and password. Only you should know your password and you must be the only person who uses your network account.

The councils have systems in place that can monitor and record all Internet usage. You should be aware that the councils' security systems are capable of recording (for each and every user) each Web site visit, each chat, newsgroup, mailing list or e-mail message and each file transfer into and out of its internal networks. The councils reserve the right to do this at any time. No employee should have any expectation of privacy as to his or her Internet usage. Managers will review Internet activity and analyse usage patterns, and may choose to publicise this data to assure that council Internet resources are devoted to maintaining the highest levels of business use and integrity.

Breach of the regulations referred to in this section may result in disciplinary action being taken against an employee up to and including dismissal. Any action against the employee will follow the councils' disciplinary procedures. Specific analysis of Internet use may be provided in support of any investigation.

A breach of the regulations or this policy may result in legal action being taken against the user.

Things You Must Not Do

Access to the following categories of websites is currently blocked using a URL filtering system:

(This list is not exhaustive and may be amended from time to time.) Some websites may not be automatically blocked by the web filter. Staff should exercise their own discretion and report any misclassifications.

- Dating
- Illegal
- Gambling
- Gaming
- Hate and Discrimination
- Hacking
- Instant Messaging
- Internet Telephony
- Offensive and Tasteless
- Peer-to-Peer Networks (These are generally used to distribute media illegally)
- Pornography and Adult Material
- Proxy Avoidance
- SMS and Mobile Telephony Services

This does not apply to EKServices ICT provided services such as web chat, instant messaging, and internet telephony.

Except where it is strictly and necessarily required for your work, for example ICT audit activity or other investigation, you must not use your Internet account to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other material that might be deemed illegal, obscene or offensive.
- Copy or modify copyright protected material downloaded from the Internet without written authorisation from the copyright holder.
- Subscribe to, enter, or use Peer-to-Peer networks or install software that allows sharing of music, video or image files. If you need further information on Peer-to-Peer networks please contact EKS ICT.
- Subscribe to, enter, or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter, or use online gaming, or betting sites.
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Run a private business.
- Download any software that has not been specifically approved for your use in advance by IT Services.
- Impersonate another person on the internet without his or her express permission.

The above list gives examples of unsuitable usage, but is neither exclusive nor exhaustive. Unsuitable material would include data, images, audio files or video files the transmission of which is illegal under British law, and any other activity that is against the rules, and spirit of this and other council policies.

Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.
- Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- Know that you may only use the councils' Internet facility within the terms described herein.
- Know that all existing council policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with privacy, misuse of resources, harassment of any kind, information and data security, fraud and the Code of Conduct.
- Remember that comments made on social networking sites, chat rooms etc. are in the public domain and must not bring the councils or their partners into disrepute, or be of a defamatory nature. The councils will not tolerate bullying or harassment of colleagues in any form, this includes via social networking.

It is the responsibility of Line Managers to ensure that the use of the Internet facility:

- Within an employees work time is relevant to and appropriate to The councils' business and within the context of the users responsibilities.
- Within an employee's own time is subject to the rules contained within this document.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Internet Use Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
25/01/2012	A Waite	1.0	Consolidation of all partners' current policies.
20/02/2012	A Waite	1.1	Inclusion of all comments and changes from the working group.
18/10/2012	Sean Hale	1.2	Document finalised.
09/01/2015	J Brackenborough	1.3	Amendments following review by policy working group.
23/09/2016	CIGG	1.4	Final Review.