Email Acceptable 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.

Email Acceptable Use Policy

Background

This policy covers all email systems and facilities that are provided by EK Services for the purpose of conducting and supporting official business activity through the network infrastructure of the organisation and all stand alone and portable computer devices.

This policy is intended for all EK Services partners and includes Councillors, Committees, Departments, Partners, Employees of the council, contractual third parties and agents of the council who have been designated as authorised users of email facilities.

Whilst respecting the privacy of authorised users, each organisation maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of email from individual accounts does not necessarily result in permanent deletion from the ICT systems. It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000.

All email prepared and sent from any official business email addresses or mailboxes, and any non- work email sent using EK Services ICT facilities is subject to this policy.

'Organisation' refers to Canterbury City Council, Dover District Council, Thanet District Council, EK Services, and East Kent Housing

Key Messages

The following list is a set of rules about the acceptable use of the organisations email system. Disciplinary action may be taken against individuals who abuse the email facility.

Users must:

- Ensure that all emails that are used to conduct or support official business of the organisation must be sent using an official email account.
- Your email account identifies you as an organisation representative, so you must be aware that the recipients of your messages will assume that you are acting on behalf of your employer.

- Make sure that you do not make any statement or comment which reflects badly on the organisation, or contradicts existing policies.

- Adopt a responsible approach to the content of emails, bearing in mind that emails often need to be as formal as any other form of written correspondence such as a letter.

- Consider whether email is the most appropriate way of communicating the message, particularly when dealing with sensitive matters or where debate is likely.

- Check your incoming email regularly, and ensure that all items that require attention are addressed within the organisations guidelines on service standards.

- Be aware that emails are disclosable in any legal action against the organisation including Freedom of Information or Data Protection requests, and emails, which have been deleted by a user or from the network, may, for a period of time, be recovered.

- Do not enter into a contract via email without following the organisations standard authorisation procedures. A contract entered into via email is likely to be legally binding in the same way as any contract, and users must be careful to avoid using language that might be construed as formally offering or accepting a contractual arrangement unless the correct authorisation procedures have been followed. If in doubt, seek the advice of the internal procurement and/or legal teams first.

- Remember that email correspondence is not private as emails can be easily copied, forwarded or archived without the original sender's knowledge. When drafting any email a user should bear in mind that it may be read by a person other than the designated recipient.

- Remember Email is not a secure medium to send confidential information. The consequences of an email containing sensitive information being sent to an unauthorised person could be a fine from the information commissioner. Other information, if mis-sent, could end up on the front page of a newspaper or be used in legal or other formal proceedings.

- Any emails containing information classified as restricted, protected, confidential or above, or which are to be sent to a GSI recipient must be sent from a GCSx email account.

- If you are away from the office for more than a day, use the system capabilities to inform message senders that you are absent and provide alternative contact points using the ‘out of office’ function, or forward your mail to other officers.

- Avoid the mass distribution/forwarding of messages, which can cause congestion on network systems, and can cause offence to some recipients.

- If you find yourself overwhelmed with unsolicited email (‘spam’), or are unsure about the validity of an email or attachment contact the ICT Service desk – it is possible to

set up controls within the email and network systems to filter out unwanted messages.

- If you need to send an email to a large number of external contacts, or you want to attach a very large document, greater than 50mb, please contact the ICT Service desk to advise them of your proposed action and/ or consider the use of a secure file sharing solution. Please bear in mind that large emails may be blocked by the recipient's email.

- A limited amount of personal use is acceptable, providing it is clear that you are communicating in a private capacity, and that you only use the system outside your working time.

- Note that the volume and content of email messages can be monitored by ICT and Audit. While this is primarily a business tool, the systems cannot distinguish between official and private email traffic, so you must be aware that any personal messages you send or receive may be viewed by other officers.

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 onto the ICT network

- Damage to the reputation of the organisation

- Users of the system using emails to bully or harass others or for some other improper or discriminatory use

- Information and data security incidents

- The propagation of unwanted Email (spam)

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

The objective of this policy is to inform users of the terms under which emails may be used by:

- Providing guidance on expected working practice.

- Highlighting issues affecting the use of email.

- Informing users about the acceptable use of ICT facilities in relation to emails.

- 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 email service.

This policy covers all email systems and facilities that are provided by EK Services for the purpose of conducting and supporting official business activity through the network infrastructure of the organisation and all stand alone and portable computer devices.

This policy is intended for all EK Services partners and includes Councillors, Committees, Departments, Partners, Employees of the council, contractual third parties and agents of the council who have been designated as authorised users of email facilities.

Whilst respecting the privacy of authorised users, each organisation maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of email from individual accounts does not necessarily result in permanent deletion from the ICT systems. It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000.

Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence and spirit of this policy before using the email facility provided for your work.
- Assess any risks associated with email usage and ensure that the email is the most appropriate mechanism to use.
- Know that you may only use the councils' email facility within the terms described herein.
- Know that all existing council policies apply to your conduct when using email , 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.
- 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 email 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**
April 2011	A Waite	1.0	First Draft of combined policies developed by EK services working group.
03/05/2011	A Waite	1.1	Amendments following client group review.
31/07/2012	A Waite	1.2	Amendments following review by policy working group
09/01/2015	J Brackenborough	1.3	Amendments following review by policy working group.
23/09/2016	CIGG	1.4	Final Review.