Cambridgeshire County Council - Email Policy Appendix D

Author:	Daniel Horrex
Contact point:	Information and Records Team, Business Intelligence Service info.security@cambridgeshire.gov.uk
Policy approval:	
Date created:	November 2017 v2.4
Date of next review:	November 2019

Contents

Part One - Introduction

1. Purpose

To inform employees and Members of their rights and responsibilities with respect to the proper use of the Council's email systems in order to protect both the Council and its employees & Members.

2. Background

The Council mandates the business use of email for all employees and Members. It therefore needs to have a formal policy regarding the appropriate use of email, and needs to inform Members, employees and managers of their rights and responsibilities associated with this use. A formal policy aids the Council in communicating appropriate procedures and in protecting against potential disclosure of sensitive information or litigation arising out of potential violations of responsibility or invasion of privacy.

3. Objective

The Council email policy is intended to allow the Council to derive the benefits of increased efficiency through the use of email, whilst ensuring the protection of information assets, reputation and integrity of the Council and employee rights.

4. Scope

This policy applies to:

- all users of the Council email system regardless of their affiliation (e.g. Council employees, Members, agency workers, contractors, partners, e.g. NHS employees);
- all Council owned or operated email systems;
- all email messages, attachments and associated files.

This policy forms part of the Council’s Information Management Policy Framework.

Part Two – Policy

5. Safe Information Handling

The Council is responsible for a wide diversity of information, including information that is in the public domain to highly sensitive personal information whose security needs to be ensured.

To manage information appropriately, staff/Members must identify the level of sensitivity of information and use this as the basis to confirm suitably secure working practices. In general, the more sensitive the information being handled, the more secure the handling and transit mechanisms required.

The Council deals with two types of information:

Official - day to day Council information such as policy documents, emails received by the organisation, processes etc. which do not require special measures to ensure confidentiality beyond standard Council practices.

Official sensitive - highly sensitive information with potential to cause substantial damage or distress to individuals or significant harm in other ways. This needs the most secure management and handling.

Official sensitive information can include personal information relating to individuals e.g. their financial position, details of cases handled by the Council, as well as Special personal information, relating to individuals' racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexual orientation, commission or alleged commission of offences or criminal proceedings involving them.

6. Use of Cambridgeshire County Council and Personal Email

Council email is more secure than personal email accounts because:

- the Council has control over the emails which it holds;
- Council email is backed up, other personal email accounts typically are not;
- the Council maintains security of the email system and mandates security controls;
- the Council controls access to the accounts whereas personal email access control is reliant on the email provider.

It is therefore the Council's policy that Council email must be used by all staff and Members for Council business unless a personal email security commitment has been agreed with the individual Member.

It is advised that a personal email account should not be used for Council business as it is unsecure and not safe. It is intended that the use for all Council email systems (i.e. @cambridgeshire.gov.uk) is for business related communication. It is advised that the personal use of Cambridgeshire County Council email is permitted in emergency occasions, personal email should be used for personal use. Technical support will not be provided for issues or problems arising from personal use of email.

Council emails must not be forwarded to a personal email account. If emails or the content of emails need to be printed then this should be done via CCC MFD (Multi-Functional Devices) which are located in CCC buildings.

Email systems and all email generated using CCC email systems, including their associated backups, are considered to be an asset owned by the Council and are not the property of any users of the Council email services regardless of whether they are employees of the Council or not.

The key principles are:

- all Members and Council staff to use their @cambridgeshire.gov.uk email address for Council business unless a Member has signed the personal email commitment statement;
- a personal email commitment statement must be signed if a member is auto-forwarding emails from their CCC email address to an alternative non CCC email account;
- all Members and Council staff to use County Council laptops/PCs, devices protected by Council security software i.e. 'Blackberry' software or County Council remote access to access CCC email accounts;
- all Members and Council staff to undertake the data protection/information governance awareness e-learning training;
- all staff to contact Members on Council business using their @cambridgeshire.gov.uk address to maintain security where the Member is using a Council email address;
- no Official Sensitive Council information should be sent to Members' personal email accounts.

If Members decide not to use @cambridgeshire.gov.uk and continue to use an alternative email account then they must accept the increased risks and liability for any security incidents involving their email accounts and sign a personal email security commitment. There are requirements set out in this agreement which mandates a number of measures to ensure that there is a decreased likelihood of their personal email account getting hacked, these include changing their password frequently and choosing a strong password.

7. Monitoring

It is the policy of the Council to monitor email messages for performance of operation, maintenance, auditing, security or investigative purposes. Full co-operation will be given to law enforcement agencies if circumstances prove necessary.

Three types of monitoring may be undertaken:

7.1 Email Filtering

The Council uses an email filtering system to screen incoming and outgoing mail (including attachments) and protect CCC systems from:

- virus attack;
- executable (.exe) files;

- spam;
- denial of service attack;
- email content deemed contrary to County Council policies regarding acceptable mail;
- prohibited file attachments such as MP3/video files that could be subject to copyright protection.

Email may be quarantined and/or deleted without the sender or intended recipient being notified.

Where this filtering system stops legitimate County Council business mail, exceptions may be made.

7.2 Manual Monitoring

Manual monitoring of email messages is not routinely undertaken. However, the Council may monitor email content if there are suspicions of misuse or excessive personal use. Any user who has the content of their mail monitored will be informed before the monitoring takes place, in accordance with the Employment Practices Data Protection Code.

7.3 Monitoring for Internal Investigations

We reserve the right to monitor email accounts in order to conduct internal investigations into allegations that the County Council's Disciplinary Rules, Codes of Conduct or Policies and Guidance have not been complied with.

In order to gain access to employee and Member email accounts, the Investigating Manager must submit a request to the Data Protection Officer explaining why the access is required, and the steps that will be taken to minimise the risk of unnecessary intrusion. Any access to staff email accounts can only be granted by the Data Protection Officer.

7.4 Monitoring of Government Connect Secure Email

Any email sent or received via GCSx* mail may be monitored and/or recorded for any lawful purpose.

* GCSx stands for Government Connect Secure Extranet and is part of the wider Government Connect initiative from central government to securely connect IT networks and share secure transport of emails and confidential data between central government and local authorities.

If no further action is taken as a result of monitoring email use, the data collected as a result of the monitoring will be destroyed immediately. Where further action is taken records will be maintained in accordance with the Council’s disciplinary procedures.

8. Mailbox Storage Limits

Storage space for large, resilient systems is costly to the Council. Therefore, to ensure the efficient running of the Exchange service, all email users must keep their mailboxes within approved limits.

Employees who have a genuine business need for a larger mailbox limit should contact the Business Support Helpdesk to discuss their requirements. Members should contact Democratic Services.

9. Access to Mailboxes

9.1 Employees with Access to Mailboxes

Network administrators and others charged with the administration, maintenance, security or operation of any Council owned system, are responsible for safeguarding employees' email messages. Normally, only the person holding an individual mailbox account has access to that mailbox. However, under certain circumstances, e.g. for support purposes, the selected staff referred to above will be able to access a user's mailbox account.

9.2 Access during Periods of Absence

9.2.1 Auto-response ('Out of Office')
It is the employee's responsibility to ensure that auto-response is switched on for periods of absence. However, line managers may request that the Business Support Helpdesk sets up an auto-response for an employee's mailbox when that employee is unexpectedly absent from work.

9.2.2 Emergency Access to Email
Emergency access to another employee's items of email without his/her express consent may only be granted at the request of that employee's Head of Service or above, who may ask that:

- specific email messages may be extracted and forwarded internally to a named employee if these emails can be identified; and/or

- all unopened and new emails may be auto-forwarded internally to a named employee.

An email will be sent to the absent employee's email account informing them of the action taken.

Once the employee returns to work it is the responsibility of the requesting department to notify the Business Support Helpdesk so that auto-forwarding can be stopped.

9.2.3 Long Term Absence
When an employee is likely to be absent for a prolonged period (e.g. maternity leave) and HR have been notified, the line manager should request that the mail account is disabled and hidden from the mailing list. Once the account has been disabled the mailbox will no longer be accessible by any other member of staff and will not receive incoming mail.

The Business Support Helpdesk will disable the accounts of employees included on the monthly HR list of long-term absentees, without a request from the line manager. Employees will be advised when this process comes into effect.

In some circumstances, e.g. during periods of secondment, the user may give permission to another named employee to access their mail account during their absence. In this case the mailbox will not be disabled. However, the named employee must undertake to manage the mailbox.

10. Mail Accounts for Agency Workers and Fixed Term Employees

Requests for accounts for agency workers are managed by the Agency Worker team. These accounts provide mailboxes which are used by the temporary worker. When the worker leaves, their mailbox is deleted.

Line managers may also arrange for Replaceable Temporary Accounts. These accounts are owned by the line manager and may be transferred to a new, temporary worker/employee complete with the existing mailbox. When the user leaves, the User Admin team should be notified, so that this account can be deleted. Before the account is transferred to a new temporary worker/employee the User Admin team must be informed and provided with the new temporary worker’s details.

For audit purposes all temporary mailbox accounts must be named accounts, i.e. contain the user’s *First* and *Last* names; e.g. firstname.surname@cambridgeshire.gov.uk.

11. Procedure for Employees Leaving County Council Employment

On notification from HR that an employee has left the employment of the County Council, the Business Support Helpdesk will disable and hide the user's mailbox account. All items contained within the mailbox at the time of disablement will be archived. The mailbox will remain hidden for a period of 30 days after which it will be deleted.

It is the manager's responsibility to ensure that any business related email is extracted before the mailbox is disabled.

12. Email Auto-forwarding

Auto-forwarding is the application of an email handling rule that enables email intended for one mailbox or recipient to be forwarded automatically to other designated recipient mailboxes. Although this may be a convenient means of transferring email data from one mailbox to another, it creates security risks i.e. personal data leaving secure IT networks and being sent to potentially insecure IT networks.

Email auto-forwarding to external accounts (i.e. outside the Council) was disabled on the Microsoft Exchange server on 31 October 2009.

Email auto-forwarding to internal accounts is permitted (e.g. from account1@cambridgeshire.gov.uk to account2@cambridgeshire.gov.uk).
This requires the approval of the appropriate Head of Service or above.

Auto-forwarding of email to or from a secure account that may contain strictly confidential information, such as a GCSx mailbox, is not permitted.

13. Confidentiality

Nothing written in an email message can be guaranteed complete privacy. Employees and Members should be aware that email messages that have been sent to others:

- can be potentially forwarded from recipients to other users of the email system;
- can be printed and ultimately read by anyone who sees the printed message;
- can be inadvertently routed to an individual other than the intended recipient (e.g. when the recipient has email delegates); and
- can be potentially accessed by others if PCs/laptops are unattended while log-in is active.

To minimise the risk of unauthorised disclosure of confidential email, all confidential messages should be flagged as such and include 'confidential' in the subject heading.

14. Security of Email Sent Beyond the County Council Environment

There are two options for sending this type of email when sending confidential/Official Sensitive information to another local authority such as Peterborough City Council or another organisation.

There are two options for sending this type of email, either:

- send or receive it between Government Connect mailboxes (GCSx accounts);
- use the Managed File Transfer tool.

Further information about safe information handling can be found in the Information Management Policy Framework or from the Safe email choices guidance.

15. Use of External Email Accounts

As external email services are not guaranteed to be secure, users must not:

- conduct County Council business via any other email service than that authorised by the County Council, unless a personal email security commitment has been agreed with the individual Member and/or
- forward mail from their County Council mailbox to any other email account that they hold.

16. Use of Government Connect Email Accounts

A Government Connect (GC) account allows access to the Government Connect Secure Extranet (GCSx) and enables communication via secure email with other local authorities and government organisations connected to the GCSx.

Restrictions on GC email accounts
There are stringent policy requirements and security restrictions that apply to all users accessing GCSx. Users must not grant other users access to their account

under any circumstances or forward GC emails to unsecured accounts or users who are not entitled to view them.

Relationship between GC secure mail and NHS mail
GC and NHS both offer a secure way to send data via email. Local authority staff should use a GC Mail account (.gcsx.gov.uk) to send and receive patient data to and from health sector staff with NHS Mail accounts (.nhs.uk).

Further information about Government Connect can be found on the County Council Intranet.

17. Publication of Email Addresses

To ensure that all email enquiries from the public are responded to promptly, wherever possible generic email addresses that are accessible by several employees should be displayed on the CCC Internet site (www.cambridgeshire.gov.uk) or on other published material.

18. Acceptable Use

Email users are responsible for all email sent from their individual accounts and should be aware of the following:

18.1 Message Content

Email system users must not send or forward mail messages that:

- contain information that could damage an individual, personally or professionally, e.g. defamatory messages; and/or
- are illegal, would be considered offensive, or would bring the Council into disrepute.

18.2 Email Addressing

The sending of email messages to the entire County Council address list is permitted but only with authorisation from the IT Client Team or Communications & Information Service. This method of addressing can lead to overloading of the email system and disrupt the service for all users, so it should be used carefully.

18.3 Emailing members of the Public

When emailing members of the public (e.g. for consultation) emails must be addressed using the 'BCC' field to prevent recipients' email addresses being disclosed unnecessarily. Great care must be taken to ensure that private email addresses are not disclosed to other members of the mail list, as doing so could breach the Data Protection Act and/or General Data Protection Regulations.

18.4 Unauthorised Access to email

Users must not access and/or store email files and messages that they are not authorised to view. Email system users must not forward mail messages and attachments that contain information that the recipient is not authorised to have access to. Users must not post or send anonymous messages, or pose as another user.

19. Retention of Email

Email communication forms part of the Council's recorded information as defined in legislation such as the Freedom of Information Act 2000. Individual communications may also form part of client files, contractual agreements and other official records. Therefore, it is important that these communications are suitable for inclusion in official records and are retrievable.

Retention of some email will be determined by policy and / or statutory requirements. Users should refer to the archiving and retention policies issued by the Information and Records Team or County Council services.

The current email system (Microsoft Outlook) and email archive should not be used for the long term storage of email. The email archive currently holds emails for 12 years before deletion, the Council will move to holding emails in the archive for 6 years to comply with Limitation act 1980. Staff and Members are advised to store outside of the email system/archive any emails which they need to retain as a formal record, e.g. saved in a network shared area.

Part 3 – Policy Application

20. Disciplinary Action

Employees and other users of the email system who wilfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to disciplinary action as determined by current HR policy and Code of Conduct.

21. Contact List

Business Support	
Business Support Helpdesk (as defined in the policy)	0300 126 7333
Information and Records Team	01223 699137 data.protection@cambridgeshire.gov.uk