Luton Borough Council

Acceptable use policy for e-Mail

Page 1 of 18

Page 2 of 18

E-mail policy

1 Introduction

This policy was written to help you understand how our e-mail system is regulated, how this affects you and what we expect from you.
Read it carefully. If you do not understand any aspect of it, seek advice from your line manager or log a call with the IM service desk on 6666. The policy covers:

- Why we need a policy.
- Who and what the policy applies to.
- The dangers that e-mails pose to the Council, its computer systems and Council employees.
- What the Council does to minimise these dangers.
- What your responsibilities as an employee are, when sending and receiving e-mail.
- The consequences of breaching this policy.

The policy has been compiled and agreed in consultation with various internal departments and with recognised union representatives. The policy meets various legislative requirements, including:

The Data Protection Act (1998)
The Human Rights Act 1998)
The Regulation of Investigatory Powers act (2000)
The Freedom of Information Act (2000)
Telecommunications (lawful business practice), (interception of communications) Regulations 2000.

2 Why we need a policy

It is important that we have an agreed set of rules (policy) on how e-mail should be used.

This policy exists:

- To protect the Council's computer systems from attack (e.g. by a computer virus).
- To highlight any pitfalls to which employees might otherwise be prone.
- To protect the reputation of both the Council and its employees.
- To detect and prevent crime.
- So we all know where we stand!

Page 3 of 18

3 Who and what the policy applies to

3.1 *Who does the policy apply to?*

The e-mail policy applies to all Luton Borough Council's employees, home workers, apprentices, students, voluntary workers, contractors, 3rd party suppliers, elected members and any other persons who have been granted legitimate access to the Council's e-mail systems.

3.2 *What does the policy apply to?*

The policy applies to the Council's e-mail systems, hardware and software and to any e-mail and content transmitted across it.

3.3 *Does the policy apply to e-mail systems hosted on the internet such as yahoo and hotmail?*

There is a separate Internet security policy, which covers this.

3.4 *Does it apply to my hand held computer or laptop, which I synchronise with Council's computer system?*

I. Yes, the policy applies to all devices that are used to access e-mail, including desktop and laptop PCs and personal organiser type devices.
II. If employees are permitted to use their own equipment for work purposes, when they connect to or synchronise with Council equipment, they become subject to this policy as if they were using Council equipment.

Page 4 of 18

4 Dangers posed by e-mails to the Council, its computer systems and to Council employees.

There are a variety of threats posed by e-mail. A few of these are listed.

4.1 Threats to the e-mail system itself

Virus attacks – malicious computer code carried by e-mail.
Denial of Service (DOS) – the flooding of the e-mail systems so that it becomes very slow or unusable.
Chain letters - often a way of passing a virus or congesting the e-mail system.

4.2 Threats to employees

Offensive or harassing e-mail.
Unsolicited Commercial e-Mail (UCE) / Spam - unsolicited mail sent to Council employees.
Attempted frauds and scams targeting employees.
Loss of reputation caused by unprofessional work practices or conduct.

4.3 Threats to the Council as a whole

Loss of reputation caused by unprofessional work practices or conduct.
Inability to authenticate facts.
Inadvertent commitment of Council funds (in an e-mail) by employees.
Attempted frauds and scams.
Other Criminal activity.

This list is not exhaustive

Page 5 of 18

5 The following steps are undertaken to reduce or remove these threats.

NB the e-mail system is a fundamental business communication tool and is the property of the Council. The Council reserves the right to access messages sent over the e-mail system to protect its computer systems or where there is an indication of a threat to the Council or its employees. Employees must not assume that e-mail content is confidential.

5.1 Accessing e-mail

The Council's methods of accessing e-mail are as follows:

5.1.1 Virus scanning

All e-mails and attachments enter the Council come via a firewall (safe connection) and are subject to virus scanning. If a virus is detected the e-mail may be cleaned, quarantined or if necessary deleted, to protect the Council's network

5.1.2 Content scanning

All e-mails sent to or received from the outside world are subjected to a threat scan. This scans the e-mail and assesses whether it may pose a threat *(See section 4 Dangers posed by e-mails to the Council, its computer systems and to Council employees).*

Content scans on Incoming e-Mail

Only if the scan determines that a message is likely to pose a threat, will it be quarantined or blocked. Messages posing a potential threat will be placed in a holding area and both the sender and the intended recipient at LBC informed of the fact.

The following message will be sent to the intended LBC recipient of the e-mail

> *A message has been sent to you by <e-mail address of sender>, Subject<e-mail title>.*
> *The message has been held for the following reason <reason given>*
>
> *You may contact the Service desk on 6666 and request either that the message is passed to your mail-box or that the message is deleted.*
> *If you do not contact the Help Desk the message will be automatically deleted after 30 days*
>
> *Service desk personnel will not review the message unless you request them to do so.*

Page 6 of 18

If you ask for the message to be passed to your mail-box you must accept that the content may be offensive, harassing, bullying, obscene or pose a threat as outlined in the LBC Acceptable usage policy for e-Mail. Please note that storing, forwarding, printing and in some cases viewing of inappropriate material is also contrary to this policy and may lead to disciplinary action.

Any annoying, abusive, offensive or otherwise inappropriate e-mail messages should be reported to the Service desk who can prevent more messages being sent from that e-mail address.

The following message will be sent to the sender of the a blocked e-mail message:

The message that you have sent to <recipient>, subject, <message title>, <Date & time> has been quarantined for the following reason <reason given>.

The intended recipient is aware of this and has the choice to either accept or to delete your e-mail.

Our apologies for any inconvenience caused, however if your message is urgent you may wish contact the intended recipient and advise them that the message has been quarantined and is awaiting collection.

Please be aware that only where there is an indication of e-mail misuse or abuse, a report may be passed to your Internet service provider.

Content scans on outgoing e-Mail

Only If the scan determines that a message is likely to pose a threat, will a message be held and the sender alerted.

The following message will be sent where an e-mail leaving LBC is held.

The message that you sent to <addressee> subject <e-mail title>, <date and time> has been held for the following reason:<reason given>

If you believe that the message has been held in error you may contact the Service desk on 6666 and request that message is released. If you do not contact the Help Desk the message will be automatically deleted after 30 days.

Guidance on why e-mails are held and on what constitutes inappropriate e-mail content can be found in the LBC e-Mail Acceptable Usage Policy

Page 7 of 18

Please note that sending of inappropriate material is contrary to the LBC e-Mail Acceptable Usage Policy and may lead to disciplinary action.

5.2 Retaining e-mails

All e-mails sent and received by the Council's e-mail system are copied to a secure electronic vault, irrespective of content. The e-mail messages held within the vault will be treated as business records by the Council and will be stored (and ultimately destroyed) in line with the Council's archiving policies and best practice i.e. for a number of years. Employees must be aware that if they delete a message from their mailbox, it does not mean that all copies of the message have been deleted.

Internal and external mail items stored in mailboxes for a period of time are archived to another section of the vault. This improves the performance of the e-mail system.

The Council has the ability to search for and retrieve archived messages (including attachments) from the vault. Any such search will only be initiated under controlled circumstances and within the authority given to the Council by the Data Protection Act and the Telecommunications (lawful business practice), (interception of communications) Regulations 2000 and the Regulation of Investigatory Powers Act (2000). In practice this means that the contents of the vault may not be disclosed without the permission of either, the Head of Human Resources, the Council's Monitoring Officer or their delegates and only if the request is made against one or more of the following criteria.

1. *To establish the existence of facts*
2. *To ascertain compliance with regulatory or self regulatory practices or procedures*
3. *To ascertain or demonstrate standards which are achieved or ought to be achieved by persons using the system.*
4. *To prevent or detect crime*
5. *To investigate or detect unauthorised use of the Council's computer systems*
6. *To ensure the effective operation of the system*
7. *In the interests of national security*

E-mail content will be retained and used for disciplinary purposes. Where action is being taken as part of a disciplinary process against an employee, copies of relevant e-mails will be obtained and used in evidence. This is in accordance with the Council's disciplinary process.

Page 8 of 18

5.3 Accessing an individual's mailbox

Where an employee is absent and it is necessary to access their mailbox to ensure that work has been or is carried out, their Head of Service may request access to the employee's mailbox by contacting the Service Desk X 6666. Access will only be granted to Line Manager as identified by the Head of Service.

Requests for access should only be made where an employee's absence is unplanned and an emergency has arisen.

If the absence is planned then the employee should either arrange to forward relevant emails to other people or set-up the facility to allow other users to view their mailbox using the Delegate facility within Microsoft Outlook. If required, guidance in using this facility can be provided by the Service Desk 6666.

This facility should not be used in relation to disciplinary matters. Instead the same information can be obtained by making a request for information from the electronic vault, where copies of all e-mails are held and which meets the required legal standards for provision of evidence.

5.4 Securing access to mailboxes

The majority of mailboxes in the Council's e-mail system are specific to individual users. To access these mailboxes you must enter a unique username and password. This is usually done as part of the log-on process when you sign on to your PC.

Some 'shared mailboxes' exist, where a single mailbox is accessed by a number of employees. Only specified employees can sign on to these using their own log-on and password.

5.5 Limiting access to external e-mail

The facility to send e-mail via the Internet is only granted to employees if requested by their Manager. The request must include a business case outlining how the external e-mail will be used and its benefits to the Council.

5.6 Limiting the size of mailboxes

In order to ensure acceptable levels of performance both on PCs and on the e-mail system mailboxes are subject to the following size limits:

- At 15mb a warning will be issued to you requesting that you reduce the size of your mailbox.
- At 20mb you will be unable to send any more e-mails until housekeeping has been done. The facility will then be automatically restored.

5.7 Deleting e-mails

Where e-mails pose a threat to the Council or its computer systems, the Council reserves the right to delete them without prior warning.

Page 9 of 18

5.8 *Limiting legal liability via a disclaimer*

This is done by the inclusion of the following footer on all e-mails sent outside of the Council.

"Luton Borough Council routinely monitors the content of e-mail sent and received by its e-mail systems, to ensure compliance with its policies and procedures.

E-mails that contain encrypted material, program files, are obscene, inflammatory, criminal, offensive, in breach of copyright or contain a virus or threat to Council's computer systems may be intercepted and/or deleted.

Internet communications are not secure. The Council is not responsible for any changes made to the message after it has been sent.

This message is intended only for the addressee. Any unauthorised copying or distribution may be unlawful.

If you are not the intended recipient, please notify the sender at Luton Borough Council Town Hall, Luton LU1 2BQ. Tel. (01582) 546000 or by using the reply option to this e-mail. Then delete this message from your system.

Website: www.luton.gov.uk"

5.9 *Employee awareness and training*

A particularly useful resource is Human Resource's paper on e-Mail etiquette, which can be found in Outlook Public Folders.

Various courses are available to employees covering e.g. PC awareness, Plain English and Microsoft Outlook use.

Articles on e-mail and other IT issues appear in LBC news on a regular basis and specific issues may be highlighted by e-Mail Bulletins to employees.

Page 10 of 18

6 Employee responsibilities, when sending and receiving e-mail.

These actions are seen as ‘best practice’ failure to follow them may lead to corrective or in some circumstances, disciplinary action.

- At all times the e-mail system must be used with respect to the dignity and privacy of others.

- Consider whether e-Mail is the most appropriate way of communicating your message. A phone call or meeting can be more effective in a number of circumstances, particularly when dealing with sensitive matters or where debate is likely.

- Check your mailbox regularly, ideally once a day.

- Respond promptly to all messages requiring a reply.

- If you are out of the office for a day or more, use the ‘out of office assistant’ in Microsoft Outlook to:
    - Alert senders of your absence.
    - Advise when you will return.
    - Give alternative arrangements in your absence.

  Don’t state that you are out of the country or on holiday
  A simple statement that you will be out of the office until a given date is better.

- If appropriate you can configure Outlook to forward mail to a colleague, or delegate permissions for them to view your mailbox. Advice on using Outlook can be obtained by logging a call to the IM service desk x6666. Outlook training courses are available through IM training.

- When sending an important e-mail internally use the options in Outlook which notify you when (a) the e-mail has been delivered and (b) the e-mail has been read. For external e-mails it may be appropriate to phone to confirm receipt.

- Review your inbox and personal folders regularly and tidy up as necessary

- Do not use uppercase in the body text of an e-mail as this may be construed as SHOUTING and can cause offence.

- Don’t use abbreviations and shorthand.

Page 11 of 18

- If you wish to e-mail a file to another employee on the LBC e-mail system, Consider using a shortcut to the file, rather than sending the file itself.

- At all times e-mails must be polite and easy to understand.

- Continued vigilance is required surrounding viruses, especially when receiving unsolicited messages. If you are in any doubt as to what the message contains do not open it, delete it. Please read the section on viruses within the PC security manual for more information on this subject.

- Never use the auto-forward option within Microsoft Outlook to forward your e-mails to a non-LBC e-mail address.

7 Definitions of e-mail misuse

E-mail misuse is likely to lead to disciplinary action.

7.1 Sharing, obtaining or attempting to obtain passwords

Do not share your passwords with anyone, including your work colleagues, or engineers working on your PC (they don't need to know it!). If you think that a password has been compromised contact the IM Service Desk immediately on 6666 and report the facts as a 'security breach'.

7.2 Inappropriate Content

Do not send or forward any e-mail content (text or attachments), which might be construed either by the recipient or by any other Council employee as:

Abusive	Bullying	Defamatory
Disruptive	Harmful to Council morale	Harassing
Insulting	Intolerant	Obscene**
Offensive*	Politically biased***	Sexual innuendo
Violent	Threatening	
** Prohibited material will include any material which may be construed as offensive on the grounds of gender, race, ethnic origin, disability, sexuality, religion, transsexualism, gender re-assignment, age, HIV status, size, stature, trade union membership/office or any combination thereof.*		
*** the use of e-mail to send, view or store pornographic content, or provision of a council e-mail address to a 3rd party with the intention of receiving pornographic content will constitute gross misconduct.*		
****As Council employees we must not demonstrate partiality for or against any political grouping or individual (this may not apply to elected members or union employees fulfilling an obligation on behalf of their constituency/union).*		
The above lists and examples are not exhaustive		

Page 12 of 18

Employees should be aware that if they send or forward e-mail containing inappropriate content, they are likely to be in breach of the Council's harassment and equal opportunities policies. Such breaches are likely to constitute gross misconduct in accordance with the local disciplinary policy and procedure.
Ask yourself before sending any e-mail "how would I feel if the content was made public"?

7.3 Libellous content

Do not make comments that could be libellous. An untrue statement, which damages the reputation of a person or organisation, or holds them up to hatred, ridicule or contempt, is libellous. The statement doesn't have not be insulting to be libellous e.g. it could allege that an organisation is in financial difficulties, losing staff or is incompetently managed. Before you send or forward any e-mail. Ask yourself, could you support the statement in court?

7.4 Breaches of Confidentiality

Material should not be circulated outside the group for which it was intended.

Do not disclose, publish or otherwise distribute another employees e-mail address without their prior consent.

Be cautious when disclosing your own Luton Borough Council e-mail address. It may be used to send you unsolicited mail.Under the Data Protection Act you can insist that your e-mail address is only used for a specific purpose and not added to any mailing lists or used for mail-shots.

Do not read, delete or copy the contents of another person's mailbox unless you have been correctly authorised to do this.

7.5 Unauthorised encryption or steganography (camouflage)

Encryption or camouflage of e-mail poses a number of threats to the Council. See section 4 'Dangers posed by e-mails to the Council, its computer systems and to Council employees'. These techniques may therefore only be applied to e-mails if they are a Council business requirement.

7.6 Creating E-mail congestion

Do not create or forward either within the Council or to external e-mail addresses; jokes, pictures, e-cards, cartoons or trivial messages.

Do not circulate or copy e-mails to persons who do not need to see them.

Do not send or forward any non-business e-mail that encourages you to forward the message to a number of other recipients such as chain letters. Common examples of chain letters are e-mails which promise improved health, wealth,

Page 13 of 18

luck or happiness to you or to others if you forward the message to a number of other recipients.

7.7 Creating a legal obligation without appropriate authority

Where e-mail is used to commit to a legal obligation or contract you must ensure that all appropriate procedures have been followed and relevant authorisations and signatures have been obtained before the commitment is made.

7.8 Running, storing or installing unlicensed software

Do not run, store or install software (other than business related demonstrations or evaluations) it unless it is correctly licensed to the Council and the installation has been authorised by Information Management.

Please read the Council's PC Security Manual for additional guidance on software installation.

7.9 Breaching the Copyright Act

The copyright act makes the unauthorised copying and distribution of software, books, movies and music illegal. If you receive a file containing software, text, audio files or movie files (other correctly licensed and authorised software as specified in the paragraph 7.8 'Running, storing or installing unlicensed software) do not open, save or install it, delete it.
NB Breaching the copyright act is a criminal offence.

7.10 Committing or abetting a crime

Use of e-mail to commit a crime or assist others in committing a crime will be classed as gross misconduct

7.11 Other actions that may be classed as misuse

- Impersonating any other person when using e-mail.
- Maliciously amending messages received.
- Deliberately introducing or forward e-mail viruses, malicious software code or otherwise undertaking any activity that might degrade the performance of the Council's computer systems or those of another organisation.
- Using e-mail to advertise or conduct non-Council business affairs from the workplace.
- Giving out your council e-mail address as a point of contact for non-council business affairs or organising social and sporting events.

8 Secure transmission of e-mail

E-mail sent over the Internet is not secure. It is possible for messages to be intercepted and read by someone other than the intended recipients. If the message is confidential a degree of protection is afforded by password protection of file attachments.

Page 14 of 18

9 Personal use of e-mail

9.1 Conditions and limitations

Use of e-mail for personal purposes is permitted subject to the following additional conditions and limitations:

- The Council provides e-mail to its employees, as a business tool. As previously stated, e-mail may be stored, intercepted, read or deleted by the Council and should not be seen as confidential.

- A personal e-mail is a message with content wholly or substantially unrelated to the sender's role within the Council and sent using the Council's e-Mail system. E-mails sent to other LBC employees, to employees of other councils or to any external recipients are included in the scope of this definition.

- If you choose to send a personal e-mail you must understand and accept that your message will be subject to a virus and content scan, as per any other e-mail message sent or received.

  If the scan determines that a message is likely to pose a threat because:

  - The e-mail is encrypted.
  - Content is obscene, inflammatory, criminal or offensive.
  - E-mail is Spam (junk mail).
  - Content contains an executable file (e.g. a game, a virus, a software application or a macro).

  The message may be held and you will be alerted to the fact (see paragraph 5.1.2 'Content Scanning').

- It is estimated that the average e-mail takes around 3 minutes to write and send. With this in mind the Council has limited the number of personal messages that an employee can send to a maximum of 10 brief messages (i.e. 1 or 2 sentences) a week.

9.2 Items wanted and Items for sale

The Items wanted and Items for sale folders in Public folders are provided for personal use. Viewing or posting advertisements in these folders is not permitted during your contracted hours of employment, other than during designated breaks. For employees on flexi time, this means you must be 'flexed-out'.

Page 15 of 18

As these folders form part of the Council's e-mail system, their contents are bound by this policy.

The council cannot guarantee the suitability, quality or safety of items advertised in the 'items for sale' and 'items wanted' folders and accepts no liability for any fault, injury or damage resulting from any product or service purchased or otherwise obtained from these folders.

- **You are reminded that all e-mail messages (including personal messages) are subject to Council policy. Any breaches of this or other Council policy will be acted upon and disciplinary action may be taken.**

10 Policy enforcement and responsibilities

10.1 Overview of responsibilities

Primary responsibility for the maintenance of this policy lies with Information Management, who will updated it in line with changes in environment, legislation and best practice. Suggestions and comments on the policy are welcomed.

Responsibility for enforcement of this policy is the combined responsibility of all employees, their managers, Human Resources and Information Management.

10.2 Manager's responsibilities

Where a manager requires access to copies of employee e-mails held within the vault they should contact Human Resources who will in turn contact Information Management and request access to copies of any e-mails sent and received by the employee(s) concerned. A reason for the disclosure must be given, which is in line with the criteria described in section 5.2 'Retaining e-mails'.

Any request must be approved by either the Head of Human Resources, the Council's Monitoring officer or their delegates.

The results will be disclosed to Human Resources in the first instance. Any subsequent disclosures will be made in line with the Council's disciplinary policy.

10.3 All staff responsibilities

Where any member of staff becomes aware of a breach of this policy they should report the matter either to their Line Manager or to the Service desk 6666. Any breaches reported via the service desk will be forwarded to Departmental Human Resources.

11 Reports

The following reports on e-mail activity will be produced on a monthly basis:

Page 16 of 18

- Aggregate reports of e-mail activity and trends, for internal and external e-mail for use by Information Management

- Aggregate reports of inappropriate content within e-mail (for external e-mail only). For use and distribution by Human Resources and Senior Management.

- Summary reports of blocked messages (including the name of the sender). For use and distribution by Senior Management.

Other reports may be produced on demand, namely:

- Specific analysis of individual e-mail messages and specific employee e-mail use will be provided in support of any investigation sanctioned by Human Resources.

This policy has been agreed with the Council's constituent trade unions. Any future amendments/ revisions will be subject to full consultation and agreement.

Signed…….Branch Secretary Unison

Date……..

Signed. ……Trade Union Co-ordinator

Date……..

Signed…….Head of Human Resources

Date…….

Page 17 of 18

Page 18 of 18