APPENDIX 'A'

AGENDA ITEM 7(A)

EAST HERTS COUNCIL

ACCEPTABLE USE POLICY FOR E-MAIL

E-mail policy

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 People and Organisational Services. 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.

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!

Who and what the policy applies to

Who does the policy apply to?

The e-mail policy applies to all East Herts 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 (Includes past and current) to the Council's e-mail systems.

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.

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 (e.g. whilst undertaking Council business).

Duty of Care

Users must take the same care in drafting an email as they would for any other communication. Please remember e-mail sent over the internet is not 100% secure.

Freedom of Information

All emails held by East Herts Council are subject to disclosure under the Freedom of Information Act 2000, in the same manner as any other written communication.

Records and Information Management

This policy forms part of the Council's overall Records and Information Management Policy.

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 Help desk Ext 2249. Any breaches reported via the Help desk will be forwarded to People and Organisational Services.

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.

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.

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.

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.

Secure transmission of e-mail

Internal e-mails are secure.
E-mail sent over the Internet is not 100% secure. It is possible for messages to be intercepted and read by someone other than the intended recipient.
If the message is confidential a degree of protection can be afforded (if required) if the message/document is created as a password protected document and attached to the outgoing e-mail as a file attachment. (The recipient will need to know the password to open the attachment).

Alternatively, Safe Haven fax (where the receiving fax machine is in a secure, controlled location) is the secure alternative without encrypted e-mail or other secure electronic method of data transmission.

This list is not exhaustive

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 to themselves and recipient.

Accessing e-mail

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

Virus scanning

All e-mails and attachments enter the Council's e-mail system 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.

Content scanning

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

E-mails will be checked for 'Anti Virus', 'Spam' and 'E-mail attachments that have unsecure content'.

Anything recognized as 'definite spam' is rejected outright and will not be allowed through.

Anything recognized as 'possible spam' is quarantined and the recipient will be notified by an automatic email. The recipient should contact the IT help desk to follow up for possible release of e-mail.

Any e-mail recognized as 'maybe spam' will be forwarded to recipient's 'Junk Mail' folder for recipient to determine.

Content scans on Incoming e-Mail

The email quarantine filter is cleared every morning, afternoon and evening as standard, it is also checked on an adhoc basis between these times if work allows.

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 IT help desk who can prevent more messages being sent from that e-mail address.

Please be aware that where there is an indication of e-mail misuse or abuse, a report may be passed to recipients Line Manager.

Content scans on outgoing e-Mail

Outgoing e-mails will be scanned for ‘Anti Virus’ and an East Herts footer will be added see “Limiting legal liability via a disclaimer”.

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

Retaining e-mails

All e-mails sent and received by the Council’s e-mail system are copied to a secure electronic archive manager , irrespective of content. The e-mail messages held in the archive manager 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.

Accessing an Individuals Archived Emails held in Archive Manager

The Council has the ability to search for and retrieve archived messages (including attachments) from the archive manager. Any such search will only be initiated under controlled circumstances and within the authority given to the Council by the Data Protection Act 1998 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 archive manager may not be disclosed without the express permission of either, the Head of People and Organisational Services or the Council’s Head of Paid Service or their delegates and only if the request is made against one or more of the following criteria.

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

Accessing Archive Manager procedure

Where a Director, Head of Service or Manager requires access to copies of employee e-mails held within the **archive manager** they should contact the Head of People and Organisational Services who will in turn contact the Network and Systems Support Manager 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 'Accessing the **archive manager**'.

Any request must be approved by either, the Head of People and Organisational Services or the Council's Head of Paid Service or their delegates.

The results will be disclosed to the Head of People and Organisational Services in the first instance. Any subsequent disclosures will be made in line with the Council's disciplinary policy.

E-mail content will be retained and maybe 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.

Accessing an individual's active mailbox

In exceptional circumstances it may be necessary to access an individual's mailbox to ensure that work has been or is carried out, their Head of Service or Director may request access to the employee's mailbox by contacting the Help Desk ext 2249. Access will only be granted to Line Manager as identified by the Head of Service or Director.

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 Help Desk ext 2249.

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 archive manager, where copies of all e-mails are held and which meets the required legal standards for provision of evidence.

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.

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.

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.

"This email and any files transmitted with it may be confidential and are intended for the sole use of the intended recipient, copyright remains with East Herts Council.
If you are not the intended recipient, any use of, reliance upon, disclosure of or copying of this email is unauthorised.
If received in error, please notify us and delete all copies.
All e-mails and attachments sent or received by East Herts Council may be subject to disclosure under access to information legislation.

Please note that the Council does not accept responsibility for viruses. Before opening or using attachments, check them for viruses.

David Frewin
Network and Systems Support Manager
East Hertfordshire District Council
Tel: 01279 655261
DDI: 01279 502158
email: david.frewin@eastherts.gov.uk
web: www.eastherts.gov.uk "

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 as required by the Corporate Customer Service Standards.

- 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 Help desk Ext 2249.

- 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.

- Do not leave “Read Receipt” switched on as this creates excessive email traffic, see above.

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

- If required save emails to appropriate work folder or database and delete from inbox.

- 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 that may not be understood by the recipient.

- Use font size 11 and font type Arial as standard.

- Do not put names in email subject box.

- The Corporate standard for signatures on emails should contain the following: Name/Job Title/Phone Number/Email Address/Web Address.

- If you wish to e-mail a file to another employee on the East Herts Councils 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.

- Never use the auto-forward option within Microsoft Outlook to forward your e-mails to a non-East Herts Council e-mail address without express permission of your Head of Service, Director and the Network and Systems Support Manager.

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 Help Desk immediately on Ext 2249 and report the facts as a 'security breach'.

E-mail misuse

E-mail misuse and/or inappropriate content may lead to disciplinary action.

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 Further clarification on inappropriate behaviour/content can be found in Schedule 2 of the Council's Disciplinary Policy & Procedure.

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 Council's disciplinary policy and procedure.
Ask yourself before sending any e-mail "how would I feel if the content was made public"?

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 to 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?

E-mail addresses

E-mail addresses are a business tool and at Head of Service level and above will be subject to disclosure.

Breaches of Confidentiality

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

Do not disclose, publish or otherwise distribute another employee's (below Head of Service) e-mail address without their prior consent.

Be cautious when disclosing your own East Herts 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.

Unauthorised encryption or steganography (camouflage)

Encryption or camouflage of e-mail by employees poses a number of threats to the Council. See '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.

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 unless on legitimate Council business.

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

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.

Running, storing or installing unlicensed software

Do not run, store or install software contained within an email (other than business related demonstrations or evaluations) unless it is correctly licensed to the Council and the installation has been authorised by the IT section.

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 than correctly licensed and authorised software) do not open, save or install it, delete it.
NB Breaching the Copyright Act is a criminal offence.

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.

Other actions that may be classed as misuse and subject to Disciplinary action

- 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 (except official EHC Social Team events).

Personal use of e-mail

Conditions and limitations

Use of e-mail for personal purposes is permitted if it is reasonable and does not interfere with work, 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 (i.e. not connected with your job or Council business) and sent using the Council's e-Mail system. E-mails sent to other East Herts Council employees, to employees of other councils or to any external recipients are included in the scope of this definition.

- If you choose to send/receive personal e-mails you must understand and accept that messages 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 (see paragraph 'Content Scanning').

- **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.**