Forest Heath • St Edmundsbury
West Suffolk
working together

(This report is a key decision. This report has been subject to appropriate notice of publication under the Council's Access to Information Rules)

WEST SUFFOLK JOINT STAFF CONSULTATIVE PANEL

29 OCTOBER 2012

JSP12/001

Report of the Cabinet Members for Resources, Governance & Performance (FHDC) and Performance & Resources (SEBC)

JOINT FOREST HEATH DISTRICT COUNCIL AND ST EDMUNDSBURY BOROUGH COUNCIL EMAIL AND INTERNET USAGE POLICY (Key Decision Reference: OCT12/05)

1. Summary and reasons for recommendation(s)

1.1 The purpose of this report is to seek Member approval for the adoption of a new Joint Forest Heath and St Edmundsbury Borough Council Email and Internet Usage Policy.

1.2 Although this is a new policy in its joint format it is fundamentally an amalgamation of the two existing Forest Heath and St Edmundsbury policies. There are therefore no major changes in the content.

1.3 To comply with the Government code of connection it is essential that, as we move forward with sharing services between the two authorities, our policies in this area are aligned.

1.4 The new Joint policy is attached as Appendix A.

2. Recommendation(s)

2.1 That the West Suffolk Joint Staff Consultative Panel recommends the approval of the new Joint Email and Internet Usage Policy; and

2.2 That any future minor/housekeeping changes required to the Internet and Email Usage Policy be delegated to the Head of Human Resources to amend, and that only major/fundamental changes be referred to Members.

Contact details	**Portfolio holder(s)**	**Lead officer(s)**
Name	Cllr. Stephen Edwards	Chris Woodhouse
Title	Portfolio Holder for Resources, Governance and Performance	ICT Shared Services Manager 01284 757230

Telephone	01638 660518	chris.woodhouse@forest-heath.gov.uk
E-mail	stephen.edwards@forest-heath.gov.uk	
Name	Cllr. David Ray	
Title	Portfolio Holder for Performance and Resources	
Telephone	01359 250912	
E-mail	david.ray@stedsbc.gov.uk	

3. How will the recommendations help us meet our strategic priorities?

3.1 N/A

4. Key issues

4.1 As the two councils move towards the sharing of services and related ICT systems it is increasingly important that relevant ICT policies and procedures are brought in line. A new joint policy for email and internet use has therefore been created as part of this process.

4.2 To comply with the Government code of connection it is essential that, as we move forward with sharing services between the two authorities, our policies in this area are aligned.

4.3 The new joint policy is an amalgamation of the existing policies of Forest Heath District Council and St Edmundsbury Borough Council. There are no major changes in content but a summary of changes that have been made are listed below:

- The tense throughout the policy has been changes to make it relate to both councils.
- A new section has been added, 5.2, to make it clear that the councils are not to be held liable for any personal transactions made whilst using the councils facilities.
- Some minor corrections have been made to reference materials and contact details.

4.4 The new policy is attached as Appendix A.

5. Other options considered

5.1 N/A

6. Community impact

6.1 Crime and disorder impact *(including Section 17 of the Crime and Disorder Act 1998)*

6.1.1 N/A

6.2 Diversity and equality impact *(including the findings of the Equality Impact Assessment)*

6.2.1 There are no direct equality and diversity issues arising from the introduction of the revised Internet and Email Usage Policy.

6.3 **Sustainability impact** *(including completing a Sustainability Impact Assessment)*

6.3.1 N/A

6.4 **Other impact** *(any other impacts affecting this report)*

6.4.1 None

7. Consultation *(what consultation has been undertaken, and what were the outcomes?)*

7.1 The new policy has been created in consultation with the communications unit, human resources, corporate policy and legal services. The relevant trade unions are being fully consulted on the new policy.

8. Financial and resource implications *(including asset management implications)*

8.1 None

9. Risk/opportunity assessment *(potential hazards or opportunities affecting corporate, service or project objectives)*

Risk area	**Inherent level of risk** (before controls)	**Controls**	**Residual risk** (after controls)
A lack of aligned ICT policies for a shared service would not meet the Government code of connection.	High	Develop joint policies across the two councils	Low

10. Legal and policy implications

10.1 This new joint policy forms part of ensuring compliance with the government code of connection for the shared ICT service.

11. Ward(s) affected

11.1 N/A

12. Background papers

12.1 N/A

13. Documents attached

13.1 The new Joint Email and Internet Usage Policy.

W:\Democratic WP Services\Committee\Reports\West Suffolk Joint Staff Consultative Panel\JSP12-001 Joint FHDC & SEBC Email & Internet Usage Policy.doc

Appendix A

Joint Forest Heath District Council and St Edmundsbury Borough Council

E-mail and Internet Usage Policy

Forest Heath • St Edmundsbury
West Suffolk
working together

Employees' Version

1. Introduction

1.1. This Policy contains important rules covering e-mail, internal and external, and access to the Internet. Many of the rules apply equally to the Councils' other methods of communicating such as letter, fax and telephone.

1.2. This Policy explains how e-mail and the Internet should be used. It explains what you are allowed to do and what you are not allowed to do.

1.3. This Policy has been drawn up by the West Suffolk ICT Team and Human Resources service. It has been agreed with West Suffolk Unison Branch and approved by Cabinet. If you have any general concerns over this Policy please contact one of these services or Unison.

2. Failure to comply

a) may result in legal claims against you and the Council; and

b) may lead to disciplinary action being taken against you, (see Disciplinary and Capability Policy and Procedures on the Intranet).

2.1. **It is vital that you ensure that you are familiar with the contents of this Policy**. If there is anything that you do not understand, it is your responsibility to ask your manager to explain. By accessing and using the Councils' internet and e-mail facilities you are acknowledging your agreement to this policy.

3. Monitoring Usage

3.1. The Council automatically monitors the level and route of e-mail and Internet traffic. Logs are kept on the system. These may be inspected at any time without notice where there is just cause for suspicion of misuse. If through routine monitoring the Council has grounds for suspecting an employee of illegal or inappropriate e-mail or Internet use further investigations, including the examination of relevant computer files, records and e-mails, may be carried out. This will include any personal files & e-mails held on council equipment and will be conducted by West Suffolk ICT staff. Investigations will be conducted in accordance with either Council's disciplinary procedure, and disciplinary action taken where inappropriate use is established.

3.2. The Councils monitor and block internet sites visited from the Councils' networks for inappropriate content. 'Inappropriate' includes, but is not limited to material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, describes techniques for criminal or terrorist acts 'and any other categories as determined from time to time by the Head of HR'. If you visit such sites, the disciplinary procedure described in 2.1 above will be instigated.

3.3. The Councils also block internet sites that are not appropriate for use at work, including internet-based email sites. If you find that a site that you need for work purposes is blocked, please contact the IT Helpdesk with details of the site to which you require access.

3.4. The Councils' networks are set up so that all external e-mail and files exchanged over the Internet pass through the Councils firewalls and filtering software to prevent the spread of viruses and malicious software.

3.5. All e-mail and attachments are scanned for viruses and inappropriate content. If any are found the e-mail is withheld. A message to that effect is returned to the sender and, for incoming mail only, to the recipient. The West Suffolk ICT Help Desk is informed of any virus or inappropriate content.

4. Security

4.1. It must be understood that e-mail is not secure and that no personal, confidential or sensitive material should be sent by e-mail without careful consideration. For example it is possible that technical staff may see isolated messages just as telephone engineers may overhear telephone calls, or a hacker may intercept an e-mail. Council staff are required to maintain the privacy and confidentiality of any message inadvertently viewed.

4.2. Since 2009, both Councils have been connected to the Government Secure Extranet GCSx which does provide a higher level of security for sensitive information. All e-mails sent via this route must follow the protective marking scheme in appendix E of the ICT Security Policy.

4.3. Users who process e-mails marked RESTRICTED must not attempt to forward them on to non-GCSx mail addresses. These will be blocked.

4.4. All e-mail is passed through the councils' spam (unsolicited or junk mail) filter. Known spam is deleted immediately, suspect spam is quarantined and checked daily by the West Suffolk ICT Help desk staff. Where suspicions have been raised, a warning is given. If you suspect that e-mails you are expecting, may have been incorrectly identified as spam, then contact the West Suffolk ICT Help desk on ext 7677 (01284) 757677 or ict.help@westsuffolk.gov.uk and appropriate advice will be given.

4.5. E-mails are subject to the Data Protection Act and the Freedom of Information Act 2000 so could be subject to requests for copies by the public. Guidance is given on the Intranet about the Act and what is covered by it and exemptions.

4.6. Mobile and home enabled workers should ensure that e-mails are not copied to non-council devices, e.g. domestic PCs or Smart Phones. Particular care must be exercised if sending and receiving e-mails when travelling outside the UK as network security standards are known to differ from those covered by UK laws & regulations.

5. General rules

5.1. The Councils' Internet and e-mail systems are primarily for business use. Occasional and reasonable personal use is permitted provided that this does not interfere with the performance of your duties. Reasonable personal use of e-mail facilities is acceptable at any time but personal use for Internet access should be carried out in your own time. The Councils' Internet or e-mail facilities must not be used for personal gain.

5.2. The Council is not responsible for any personal transactions you enter into - for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from your transaction - for example in relation to payment for the items, data loss or any personal injury or damage to property they might cause. If you purchase personal goods or services via the Council's Internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Council.

5.3. The use of web based e-mail services such as Microsoft Hotmail is prohibited, as this bypasses the Councils' full security system. All e-mail should be sent/received using the corporate e-mail system.

5.4. For external emails, the Council system will automatically add a Council disclaimer. However, if you send a personal e-mail sign off the e-mail with the following statement:

PERSONAL E-MAIL*: This e-mail is personal. It is not authorised by or sent on behalf of the sender's employer. This e-mail is the personal responsibility of the sender.*

5.5. E-mails are not to be sent nor Internet pages accessed if the contents are likely to be illegal, could bring either Council into disrepute or could make the Councils liable to action against them. Examples include material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, describes techniques for criminal or terrorist acts or otherwise represents values which are inappropriate to the Council's activities or could bring the Council into disrepute.

5.6. Access to another person's e-mail is only allowed with the authorisation of the mailbox user or the West Suffolk ICT Shared Services Manager. Technical staff must not deliberately access another person's e-mail without authorisation. All passwords should be kept secure.

5.7. Staff should not:

- bypass, or attempt to bypass, the Councils' security controls.
- send viruses or hack into any e-mails or computer systems of the Councils or other organisations.
- send or forward chain letters or unsolicited mail (spam).
- impersonate any other person (for example, by using another's password) when using e-mail and do not amend messages received.
- introduce software or any electronic media onto the Councils' systems without the prior permission of the West Suffolk ICT Team. This includes software, shareware and freeware available on the Internet.
- subscribe to any bulletin boards, newsgroups or any other Internet service of any kind whatsoever without prior permission from their line manager.

6. Good practice in using email

6.1. The Councils are as liable for the advice or content given in an e-mail as they are by any other means of communication. Use appropriate language, as you would for formal written material. (old para 5.9) You may wish to ask yourself, before sending an e-mail, how you would feel if your message were read out in court. E-mail messages may have to be disclosed in litigation.

6.2. Do ensure that your use of e-mail complies with the Freedom of Information Act. Staff Guidance notes can be found on the Intranet or are available from Human Resources.. Your Head of Service can supply you with a copy if you don't already have one.

6.3. Take care about the style you use, be friendly, businesslike and brief but not curt.

6.4. Do not use **bold** or UPPER CASE lettering unnecessarily. This is known in e-mail terms as shouting. Also, avoid lengthy upper case text and underlined text (unless it is a link) for accessibility reasons as this can be difficult to read.

6.5. Obtain confirmation of receipt (for example, asking the recipient to send an e-mail reply) for important e-mails sent. Don't rely on 'view acknowledgements' as this is not supported on all e-mail systems.

6.6. Keep copies of important e-mails sent and received. Advice on how to store these in appropriate folders is given on email storage guidance and setting up an archive on the intranet.

6.7. Check your e-mail regularly, at least once each working day.

6.8. It is good practice to make arrangements for your e-mail to be forwarded to, or accessed by, someone else in your absence. If you don’t, it may be necessary to gain authorisation to access your mailbox when you are absent. Use the ‘Out of Office Assistant’ under Tools in Outlook to inform senders and use it to make arrangements for your e-mail to be forwarded as appropriate. If you do not put other arrangements in place, it may become necessary for the Council to access the contents of your mailbox if you are absent from work for any reason.

6.9. Reply promptly to all e-mail messages requiring a reply. Where a prompt detailed response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when a detailed response will be sent.

6.10. Do not create e-mail congestion by sending copious trivial or personal messages or by copying e-mails to those who do not need to see them.

6.11. Acknowledge Internet derived material in Council documents. See also Copyright below.

6.12. Do not access the Internet for purposes other than those for which you are employed unless in your own time.

6.13. Do not deliberately visit, view, or download any material from any website containing sexual or illegal material or material which is offensive in any way whatsoever.

If you accidentally visit a site with inappropriate content or receive inappropriate e-mails, immediately inform your manager or the West Suffolk ICT Help Desk on ext 7677 (01284) 757677 or ict.help@westsuffolk.gov.uk

7. Problem Areas

Harassment

Liability for harassment of colleagues by e-mail or the distribution of sexually explicit or racially offence material, or material offensive to those with a disability, could rest both with the employee and also with the employer. The employer will also be liable for acts by a third party if the employer could have controlled the situation.

Defamation

Inflammatory or derogatory messages sent through the Internet can be held to be defamatory if the message is likely to be available to readers other than the employee and the recipient. A defamed party personally could sue the employer and the employee for large sums in damages. Criminal penalties could also apply.

Copyright

Copyright laws protect most material appearing on the Internet and some attachments to e-mails. Both the employer and the employee could be liable under civil and criminal law for any unauthorised copying of those materials by the employee.

Entering contracts

An employee can easily commit the employer to binding contractual obligation by e-mail, just as by letter, fax, telex or telephone. It has become popular for parties to contract by e-mail or the Internet using electronic or digital signatures. The Electronic Communications Act 2000 conveys the same legal standing for digital signatures as a normal signature on paper. Great care will be needed to avoid forming contracts where employees have access to electronic signatures. For further advice, contact the Finance/Procurement.

Pornography

Displaying on screen, storing, printing or transmitting material with a sexual content could constitute criminal offences for which both the employer and the employee are liable. However, regardless of any criminal investigations or proceedings, any activity of this nature will be considered misconduct or gross misconduct and be dealt with in accordance with the Disciplinary Procedure.

Confidential information

E-mails are not necessarily a secure way of sending information. Not only could it be embarrassing for the organisation if sensitive or confidential information of its own is publicly disclosed, but disclosure of a third party's confidential information, for example that of a client, could expose the Councils to negligence actions and commercial risk. If you need to send confidential or sensitive data or information, then you should consider using GCSx. If you require access to this facility, you can get advice from your line manager or the West Suffolk ICT Help Desk on ext 7677 (01284) 757677 or ict.help@westsuffolk.gov.uk

8. Amendments

The Councils may, in consultation with Unison, amend this Policy at any time and users will be notified of any changes made.

9. What to do next

1. Print, sign and date page 6 of the Policy.
2. Copy the signed Policy.
3. Send the original signed page to HR.
4. Keep the copy handy for reference purposes.

Comment [c1]: Is this stil required?

Agreement

I have read through and understand the terms of the Email and Internet Policy and agree to abide with the guidelines therein.

Name	***Department***
Signature	***Date***

W:\Democratic WP Services\Committee\Reports\West Suffolk Joint Staff Consultative Panel\JSP12-001 Joint FHDC & SEBC Email & Internet Usage Policy - Appendix A.doc