Agenda Item

Walsall Council

Standards Committee – 26 March 2007

Email and Internet Usage Policy

Portfolio: **Cllr Longhi**

Service Area: Strategic Transformation

Wards: **All**

Summary of report

This policy explains what councillors, employees, authorised agents and partners must do when they apply to become users of the council's email and Internet services, send and receive emails and use the Internet and the council's intranet. The policy also explains how the council will monitor email and Internet usage, and any circumstances under which certain officers are allowed to operate outside this policy.

A number of investigations have taken place within the council resulting from alleged misuse of the council's email and internet facilities. During these investigations, the internal audit service and have identified that there were omissions and/or inconsistencies in the coverage provided by the existing procedure to regulate employee access to electronic communications, including email and the internet. This procedure was last updated in September 2001 and required amendment. In addition, more employees are using the Internet and email to undertake council business and an amended policy was required to provide clarification for all users in what they can and cannot do when using the council's email and Internet services.

The new policy attached at **Appendix A** has been created using best practice from other councils and the private sector. An implementation plan is attached at **Appendix B.**

The Policy was approved by the Strategic Leadership Team (SLT) on the 15 March 2007. It was also discussed at the Employee Relations Forum, including Union representation, again on the 15 March 2007. The GMB Union expressed concern about the detail surrounding the consequences of misuse. This concern was noted but the policy was agreed by the majority of the forum.

Changes to policy and procedure

The following are the major changes included in the document.

- Councillors, authorised agents and partners are now included within the policy.
- The use of internet and email were separated into discreet sections within the policy to ensure that users, who use only one or both of these services, understood the implications, for each service.
- Reference to external emails has now been removed from the policy. The new policy includes the circulation, distribution and use of internal emails.
- Reference to the use of online gaming and blogs is now included.
- Reference to purchasing via email and internet is now included.
- Accountability when creating content for the internet or email is now included.
- The management and use of generic email boxes has now been added.
- Contribution to notice boards, information sites, forums and newsgroups is now permitted in the council's name for council purposes.
- The consequences of misuse are now indicated.

Recommendation

That the Standards Committee approves the new Email and Internet Usage Policy and the implementation plan.

Resource and legal considerations

Financial
Existing systems, resources and communication channels would be used to implement the policy.

People
The new policy was created by the internal audit service, strategic transformation team, HRD, Legal Services and ISS.

Legal
Officers from legal services were consulted on the new policy. The new policy will reduce the amount of legal advice required to support the policy and any potential disciplinary actions that result from misuse of council services.

Citizen impact

The policy will support improving the quality of email and Internet services by improving the way we receive and respond to customer enquiries.

Environmental impact

N/A

Performance and risk management issues

Risk Management
A risk assessment is attached at **Appendix C**.

Performance Management
The cost of officer time in investigation/undertaking disciplinary action as a result of misuse of email and internet usage will recorded and reported. A comparison of 2006/07 and 2007/08 disciplinary data will be made at the end of year one to ensure that the revised policy implementation has been successful and any efficiencies recorded.
It will also support our vision of excellence – by providing managed email and Internet services.

Equality implications

N/A

Consultation

The new policy has been created following consultation with internal audit, strategic transformation, HRD, ISS, corporate policy and legal services. The new policy will be further consulted at the Employee Relations Forum on 15 March 2007.

Background papers

Report to SLT dated 15 March 2007 (including Email and Internet Usage Policy, implementation plan and risk assessment).

Signed:

Assistant Director
Bhupinder Gill

Date: 16 March 2007

Contact officer

Jo Stewart
Transformation Manager
☎ 658403
✉ jo.stewart@walsall.gov.uk

Dave Blacker
Chief Internal Auditor
Internal Audit Service
☎ 652831
✉ BlackerD@walsall.gov.uk

Appendix A

Walsall Council

Email and Internet Usage Policy

Description

This policy explains what councillors, council officers, authorised agents and partners must do when they apply to become users of the council's email and Internet services, send and receive emails and use the internet and the council's intranet. The policy also explains how the council will monitor email and Internet usage, and any circumstances under which certain officers are allowed to operate outside this policy.

Contacts
Jo Stewart
Strategic Transformation Team
Jo.stewart@Walsall.gov.uk

Steve Osborne
Internal Audit Service

Walsall Council
WS1 1TP
OsborneS@Walsall.gov.uk

Published March 2007
Review date 1st March 2008

Contents

Walsall Council

Email and Internet Usage Policy

1 Approval

1 The policy has been approved in accordance with the process approved by the council's strategic leadership team on 15 March, 2007. All changes to the policy will be agreed by that team and be shown on the council's intranet site. All Walsall councillors, council officers, authorised agents and partners will be informed of the document's existence and sign up to the revised policy.

2 A copy of the policy is available on the council's intranet, and is also found in the "Communications Toolkit".

2 What does the policy cover?

1 This policy explains what councillors, council officers, authorised agents and partners must do when they:

a) Apply to become users of the council's email, internet and Intranet services,

b) Send and receive emails using the council's email services,

c) Use the Internet and council's intranet, and

d) Send email, text and other data from a personal computer, mobile telephone or Blackberry type device.

2 It also explains how the council will monitor email and Internet usage, and the circumstances under which certain council officers are allowed to operate outside this policy.

3 To whom does the policy apply?

1 This policy applies to all Walsall councillors, council officers, authorised agents and partners.

2 It also applies to the council's schools as explained in Section 9.7 of this policy.

4 Legislation and council policies

4.1 Legislation

1 All users must have full and proper regard for the law, council policies and standards.

2 This policy intends to assist all users to comply with the law, especially;

a) Data Protection Act 1998,

b) Privacy and Electronic Communications (EC Directive) Regulations 2003

c) Human Rights Act 1998,

d) Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,

e) Regulation of Investigatory Powers Act 2000, (RIPA),

f) Copyright Designs and Patents Act 1988,

g) Freedom of Information Act 2000,

h) Race Relations (Amendment) Act 2000,

i) Computer Misuse Act 1990, and

j) Disability Discrimination Act 1995.

4.2 Council policies

1 All users must comply with council policies and standards, especially regarding;

a) Equality and diversity,

b) Race equality,

c) Equal opportunities,

d) Disability equality,

e) Whistle blowing,

f) Members' code of conduct,

g) Financial and contract rules and procedures,

h) Code of conduct for employees and

i) Records management policy and retention guidelines.

2 Users are responsible for ensuring their use of emails and the Internet complies with these and other relevant council approved policies.

5 Becoming a user of the council's email and Internet services

5.1 Entitlement

1 All councillors, council officers, authorised agents and partners are given access to email, Internet and intranet services only after completion of an authorised request form.

2 All Walsall councillors, council officers, authorised agents and partners of Walsall Council, are entitled to use email, Internet and intranet services for the council's business purposes where permission has been provided by the Assistant Director responsible for Information technology.

3 Walsall Council officers are entitled to use the Internet for business and private use providing it conforms to the requirements of this policy.

4 Councillors are entitled to use emails, Internet and intranet at any time providing it is not prohibited by this policy.

5 Email can be used by council officers, authorised agents and partners for private use during work time providing its use is reasonable, not excessive, does not distract users from undertaking their duties and is compliant with this policy.

5.2 Applying to become a user

1 All councillors, council officers, authorised agents and partners who wish to use email and the Internet must apply to the council's Assistant Director responsible for Information technology for this using a request form.

2 An Executive Director, Assistant Director or Head of Service must authorise the form to confirm that the requester has legitimate need for the services.

3 Councillors must complete a request form in a format approved by the council's Assistant Director responsible for information technology, and send it to the council's Monitoring Officer for certification.

4 By signing the request form, either in manuscript or by way of electronic signature, all users of the council's email, Internet and intranet services agree to be bound by this policy's requirements. This shall include an agreement that the council shall:

a) Undertake monitoring of councillors' emails, intranet and Internet usage to the extent that may be determined by the Monitoring Officer, and

b) Undertake monitoring of all other users' emails, intranet and Internet usage to the extent that the Chief Internal Auditor deems appropriate.

Monitoring will be undertaken in accordance with Section 8 of this policy.

5.3 Security

1 Every user must use a personal user identification and password.

2 No user must attempt to access emails, the intranet, or the Internet except with the user identification and password issued to them. They must not create other names or aliases.

3 All passwords are to be kept in confidence and changed using procedures laid down by the council's Assistant Director responsible for information technology and shall be made available to users through the intranet.

4 Passwords must never be disclosed to another person nor should disclosure be sought.

5 Passwords must not be written down or left where other people may obtain access to them.

6 All users shall be solely responsible for the emails sent by them and for their use of the Internet undertaken under their password.

7 All users must comply with the council's information security policy.

8 All Officers are responsible for making arrangements to ensure that emails are received by another officer during periods of absence. They should use a procedure approved by the council's Assistant Director responsible for information technology.

5.4 Withdrawal of service

1 Use of the council's email, intranet and Internet services may be withdrawn at any time, at the direction of the council's Chief Internal Auditor, Executive Director, Assistant Director or Head of Service or by an officer acting on their authority.

2 The council's email and Internet services will be withdrawn immediately from all users when they cease to be Walsall councillors, council officers, authorised agents or partners.

3 Managers must inform the ISS customer service desk when users cease to be council officers, authorised agents and partners. The council's Monitoring Officer must inform the ISS customer service desk when users cease to be Walsall councillors.

4 Email and Internet services will be withdrawn if abused or misused. Employees not adhering to this corporate policy could face disciplinary action, not excluding dismissal.

6 Sending and receiving emails

6.1 Responsibility

1 Councillors and officers can send and receive personal and council business emails providing they do not break the requirements of this policy.

2 The council's officers, authorised agents and partners are permitted to send or receive personal email providing they comply with the requirements of this policy and it is not;

a) Undertaken for profit,

b) Used excessively, frequently or unreasonably during their working hours, and likely to distract officers from their duties.

c) Likely to cause annoyance, or

d) Contain material that has the potential to embarrass the council or bring the council into disrepute.

3 Email is not a confidential means of communication. Nothing must be sent in an email, which the sender would not be prepared to say in a public place. For example email messages can be:

a) Released in response to a Freedom of Information request, Environmental Regulation request, Data Protection request or during a disciplinary hearing or legal action.

b) Intercepted by third parties.

c) Inadvertently addressed.

d) Forwarded accidentally. or

e) Forwarded by initial recipients to third parties.

4 Councillors, council officers, authorised agents and partners are solely and individually responsible for their use of email and for maintenance of their mailbox.

5 A councillor or council officer may give access to his or her mailbox to another officer or councillor providing;

a) Both of the councillors or council officers concerned have given their agreement in writing to this action,

b) The council's Assistant Director responsible for information technology has been informed in writing via the ISS customer service desk, and

c) Where email is sent on another person's behalf, the identification of both the sender and the person on whose behalf the email is sent shall be shown on the mail message.

6.2 Email security

1 A council approved, supplied and installed computer virus protection application must be installed on every machine used for emails owned by Walsall council. This must be in force at all times and be kept effective by regular update and review.

2 Officers using external systems to access email for council business use must have reasonable anti virus software and security in place and conform to the council's home working policy.

3 Any file received, which is believed to be infected with a computer virus or other malicious software must immediately be reported to the ISS customer service desk at the earliest opportunity. The council's information technology officers' advice must be followed regarding action to be taken.

4 Computer viruses can have a serious impact on business systems and records of our transactions with citizens. Users must protect themselves from a suspected virus by being wary of any unknown emails. Users must read the email title and if the author is not a potential customer or is unknown to the user the email must be deleted. Email message attachments must also be deleted.

5 A disclaimer must be added to the signature to all emails. The disclaimer below is the current standard approved. All users must add this disclaimer to every email which is being sent outside of the council.

> "The information in this message must be regarded as confidential and is intended for the addressee only unless explicitly stated. If you have received this message in error it must be deleted and the sender notified. The views expressed in this message are personal and not necessarily those of Walsall Council unless explicitly stated. Please be aware that emails sent to or received from Walsall Council may be intercepted and read by the council to ensure compliance with council policies or regulatory obligations, or for the purposes of essential maintenance or support of the email system. You should also be aware that any email may be subject of a request under Data Protection, Freedom of Information or Environmental Information legislation and therefore could be disclosed to third parties".

6 Encryption or compression of email, such as creating Zip files, must take place in accordance with instructions provided by the council's Assistant Director responsible for Information Technology through the ISS customer service desk.

6.3 Email received

1 Any email received, which is of an inappropriate nature, must be deleted at once and not distributed to anyone else. This includes, but is not limited to jokes, chain letters and messages of a pornographic, racist, sexist, unlawful or defamatory nature. Users not adhering to this corporate policy could face disciplinary action, not excluding dismissal.

2 Unsolicited offers to subscribe, unsubscribe, add or remove a user's name from a mailing list are to be deleted.

3 Downloading of files attached to emails for legitimate council business is allowed providing:

a) The council's virus scanning software is used to check for embedded viruses,

b) Wherever viruses are believed to exist, the file is not brought into any council equipment,

c) Large files that are 20 megabytes in size or greater are downloaded following advice from the ISS helpdesk.

6.4 Generic mailboxes

1 Where an Executive Director, Assistant Director or Head of Service wishes to create a generic mailbox for receiving or sending emails, they must apply for access from the ISS helpdesk.

2 The generic mailbox must be:

a) Administered by no less than two council officers, who shall agree to comply with the requirements of this policy,

b) Managed by a named council officer, who should monitor use of the mailbox and track the response to enquiries from officers, and

c) Used only for the council's business.

3 Where emails are sent from a generic mailbox, their content must be restricted to the council's business.

6.5 Sending email

1 All emails must have full regard to the confidentiality of the council's and other people's information:

a) Emails' contents shall include only information, to which the sender has the authority to access and to pass on to other people, and

b) Emails must not be used to send confidential or sensitive information to people or organisations to whom it should not be disclosed,

2 Unauthorised disclosure in Emails of the council's or other people's confidential or sensitive information, will be regarded as misconduct, including gross misconduct.

3 Full compliance with the copyright of any material sent or received via email must be adhered to. This includes, and is not limited to software, text, images, sound and video.

4 Sending, which shall include forwarding or distributing, of frivolous, abusive or defamatory messages may break the law or may harm the council's interests. This includes, but is not limited to messages which contain jokes, chain letters along with messages which are obscene, racist, sexist, ageist, pornographic, likely to cause offence to others or in breach of this policy. Action may be taken against any user not adhering to this corporate policy. Dependent on the severity of misuse, council officers, could face disciplinary action, not excluding dismissal.

5 The audience of an email must be considered carefully and the automatic forwarding of all messages to long circulation lists must be avoided to reduce email traffic and the time spent dealing with irrelevant correspondence.

6 Where any user receives an email for which they are not the intended recipient, they should:

a) In the case of frivolous messages or unsolicited offers make no reply,

b) In the case of messages which are obscene, racist, sexist, ageist, pornographic, likely to cause offence to others or in breach of this policy, report these to their line manager and then to the ISS customer service desk. The Assistant Director responsible for information technology, or an officer nominated by the Assistant Director, will liaise with the Chief Internal Auditor to determine the action to be taken, and

c) In the case of information inadvertently or mistakenly sent to them, inform the sender.

7 Users should neither use nor pass on any sensitive or confidential information sent inadvertently or mistakenly to them.

8 Users must not send emails to all staff unless absolutely necessary. The intranet or alternative communication tools must be considered before distribution.

6.6 Purchasing by email

1 The council's email is not to be used for the ordering or purchase of goods, works or services for the council, except where this has been agreed in writing by the council's chief finance officer. Where such agreement has been made, a procedure set out by the chief finance officer in agreement with the chief internal auditor shall be used in accordance with the council's financial and contract procedures rules.

2 Council officers, authorised agents and partners shall not use the council's email service to purchase any item for their own private use as this may lead sellers to believe they are entering into a contract with Walsall Council.

6.7 Retaining email

1 Some emails may contain information that needs to be retained as a corporate record of a decision or transaction. As a result, email messages must be treated in the same way as other records of business activities and must be identified and retained in accordance with the council's corporate records management and retention guidelines, which are available on the intranet.

2 The Freedom of Information Act requires the council to respond to all requests for information from anyone, regardless of the format of the information, including email within twenty working days. The council's Freedom of Information Officer's advice should be obtained prior to replying to any email identified as such a request.

3 Emails should be retained only as long as they are needed as a corporate or personal record. Other, unwanted, emails should be deleted on a regular basis.

6.8 Legal Documents

1 Except where the council's Assistant Director for Legal Services gives prior written approval, the council's officers shall not send or receive by text or email formal legal documents of the council. Where draft documents are received or sent in this way, hard copies shall be exchanged and these hard copy documents form the legally binding documentation.

7 Using the Internet

7.1 Internet Access and Security

1 All access to the Internet using equipment supplied by the council is to be made through the council's Internet service supplier and by the use of the server or modem designated and approved by the council's Assistant Director responsible for information technology.

2 The latest available version of the council approved, supplied and installed virus protection application is to be in use at all times. Any file infected or believed to be infected with a virus or other malicious software must be reported at the earliest opportunity to the council's Assistant Director responsible for information technology through the ISS customer service desk for investigation and eradication.

3 No attempt is to be made by councillors, council officers, authorised agents and partners to disable, defeat or circumvent council firewalls or other network security facilities.

4 Internet connections using the council's telephone network are not allowed.

7.2 Using or contributing to the Internet

1 Councillors can use the internet for private or council business providing they do not break the requirements of this policy.

2 Where a councillor's use of Internet services is considered inappropriate, the matter will be brought to that councillor's attention through the council's Monitoring Officer. The council reserves the right to its Chief Executive in consultation with the Monitoring officer and the leaders of political groups to withdraw services from any councillor who has made improper use of the internet under the conditions of this policy.

3 The council's officers, authorised agents and partners are permitted to use the internet for council use and personal use providing they comply with the requirements of this policy and it is not;

a) Undertaken for profit,

b) Used excessively, frequently or unreasonably during their working hours, and likely to distract officers from their duties.

c) Likely to cause annoyance to councillors, other officers or recipients, and

d) Used to access material that has the potential to embarrass the council and bring the council into disrepute.

4 Where council officers, authorised agents and partners make inappropriate use of internet services and websites including, but not limited to creating, accessing, distributing or storing pornographic, racist, sexist, or defamatory material, this is prohibited and employees not adhering to this corporate policy could face disciplinary action, not excluding dismissal.

5 Unless permission has been obtained from the council's Assistant Director for information technology, users are not permitted to use the council's IT services to create an online diary, a web log or 'blog', even if the user is doing so in their own time. Council officers developing or keeping a 'blog' without permission could face disciplinary action, not excluding dismissal. 'Blogging' refers to the development of an online diary, journal or weblog which enables users to contribute to or view regular updates within the journal or online diary. The activity of updating or contributing to a blog is called blogging and a creator of a blog is called a blogger.

6 Officers contributing to an online diary or 'blog' may face disciplinary action, not excluding dismissal if this is done frequently, undertaken during work time, or is defamatory to the council.

7 Following agreement with their line managers, council officers, authorised agents and partners of the council may contribute to notice boards, information sites, forums, and newsgroups in the council's name for council purposes, providing the content is not defamatory or bring the council into disrepute.

8 Playing games over the Internet is not to be undertaken through the council's services.

9 All council officers must refrain from political advocacy and/or the endorsement of commercial products or services when using the council's email or internet services.

10 Unnecessary or excessive Internet usage is to be avoided. This causes network and server congestion, slows other users, and ties up printers and other shared resources.

11 All Internet usage must be conducted honestly, respecting copyrights, software licensing rules, and intellectual property rights as in other business dealings and adhere to other council policies. Dependent on the severity of misuse, council officers not adhering to this corporate policy could face disciplinary action, not excluding dismissal.

12 Unlawful Internet usage is forbidden.

13 If when using the Internet, the user receives "screen pop ups" offering services or advertisements, they must close the screen and inform the ISS customer service desk.

14 Internet facilities must not be used to break the law. Use of any information technology resources for illegal activity is grounds for gross misconduct and the council will co-operate with any law enforcement agency in such situations.

15 No user shall deliberately use the council's Internet or intranet facilities to propagate any virus, worm, Trojan horse or trap-door program code or other malicious software.

16 The council's officers, authorised agents and partners must not use the council's web services to access personal Internet email providers without initial advice and written approval from the council's Assistant Director responsible for information technology.

7.3 Creating content for the Internet or intranet

1 Any service creating content for the Internet, council's website (www.walsall.gov.uk) or the intranet must ensure that the information created is properly managed and monitored for accuracy and currency. This includes the responsibility for maintaining contact information and content.

2 Special care must be taken to maintain the clarity, consistency and integrity of the council's corporate image and brand. Guidelines and further advice can be obtained from the web team (webteam@walsall.gov.uk).

3 The council's officers, authorised agents and partners must take care when creating content for the Internet, website or intranet to ensure that information is not defamatory to the council.

4 Creation of material which is obscene, racist, sexist, ageist, pornographic, likely to cause offence to others or in breach of this policy will be grounds for gross misconduct and the council will cooperate with any law enforcement agency in such situations.

5 No software or data owned by or licensed to the council is to be uploaded without explicit authorisation from the council's Assistant Director responsible for information technology, or from the manager responsible for the software or data.

7.4 Downloading material from the Internet

1 All users must comply with the copyright of any material downloaded from the Internet in accordance with section 4 of this policy. This includes but is not limited to software, text, images, sound and video.

2 Council officers, authorised agents and partners must only download software with the prior written approval of the council's Assistant Director responsible for information technology.

3 Users downloading any communications intensive operations including; large file transfers, video downloads, mass emails) must do so outside core times following advice from ISS. Video and audio streaming technologies represent significant data traffic, which often causes local network congestion.

4 Video and audio material downloaded must be for the council's use only.

5 Before downloaded files are run or accessed, they must be scanned for viruses, using memory-resident or network computer virus checking software. The council's Assistant Director responsible for information technology must be consulted before any software is downloaded from the Internet onto the council's network services. Any downloaded software must be for direct business use, be properly licensed and immediately added to Directorate inventories and asset registers. No pirated software or data may be downloaded or distributed.

6 All files downloaded from the Internet remain the intellectual property of their creator or current owner. All material uploaded to the Internet shall become the intellectual property of the council unless otherwise agreed by the council's Assistant Director responsible for information technology or Monitoring Officer.

7 Internet facilities must not to be used to download entertainment software or games. Neither shall it be used to download material which is obscene, racist, sexist, ageist, pornographic, likely to cause offence to others or in breach of this policy.

7.5 Purchasing over the Internet

1 Council officers must not use the Internet for the ordering or purchase of goods, works or services for the council's use, except where the council's chief finance officer has agreed this in writing. This is because sellers may be lead to believe they are entering into a contract with Walsall Council. Where such agreement has been made, a procedure set out by the chief finance officer in agreement with the chief internal auditor shall be used.

2 Council officers, authorised agents and partners must not use the council's internet services to purchase any items for their own personal use.

8 Monitoring of email and Internet usage

8.1 General requirement to monitor

1 The council will undertake regular monitoring of Internet and email usage in order to:

a) Protect the council's business interests,

b) Safeguard the efficiency and integrity of services provided,

c) Plan future communications requirements, and

d) Ensure compliance with this procedure.

2 Monitoring and interception of electronic communications will be undertaken in accordance with Section 5.24 of this policy.

3 Monitoring and interception systems will be used to analyse the use of:

a) The council's intranet and Internet sites,

b) The identity and amount of use made of other Internet sites accessed,

c) Internal email, and

d) External email.

4 The results of general monitoring exercises shall be disclosed only in accordance with the requirements of the law and council policies.

8.2 Monitoring individuals' activity

1 Detailed analysis of an individual's use of the Internet and/or email will only be carried out following a formal request to the council's Chief Internal Auditor.

2 These officers shall first determine whether there is sufficient reason for an investigation to take place, and in particular whether there appears to have been;

a) A breach or breaches of the law,

b) Disregard for the council's policies, or

c) Any other activity that may bring the council into disrepute.

3 Where the council's Chief Internal Auditor instigates an investigation, he shall examine or ask others to examine to the extent he considers necessary:

a) Emails – whether internal or external,

b) Intranet and Internet pages, along with any items downloaded, and

c) Files and other records held electronically, whether or not created from Emails or Internet pages.

4 In conducting such an investigation, the Chief Internal Auditor, or any officer acting on his behalf shall be given full and prompt access to:

a) Computers or peripheral equipment where owned by the council, held or stored on its premises,

b) Removable media, and

c) All items stored on the council's network.

5 The Chief Internal Auditor shall ensure;

a) All routine and investigatory monitoring activities are carried out in accordance with the agreement made by users in accordance with Section 5.24 of this policy,

b) Details of all internet sites visited, names of Email correspondents, and contents of Emails are used only for the investigation or as part of a subsequent disciplinary process, and

c) The police are informed wherever serious breaches of the law are suspected,

6 Officers shall cease examination immediately upon their discovering or holding reasonable suspicion of:

(i) Child pornography, whether as pornographic images or other material. or

(ii) Digital files that may be required for use as evidence and become contaminated by further examination or other actions.

In these cases, the matter is to be passed to the police at the earliest opportunity.

8.3 Agreement

1 By signing the access request form, councillors, council officers, authorised agents and partners agree that their use of email facilities and the Internet may be monitored.

2 Signing the access request form shall also provide consent for the Chief Internal Auditor to undertake detailed examinations of Email and internet usage as set out in section 8.2 above.

9 Roles and responsibilities

9.1 Assistant Director responsible for information technology

1 The council's Assistant Director responsible for information technology shall have overall responsibility for the provision of corporate email, Internet and intranet services, and shall:

a) Provide a corporate infrastructure to support the service including systems to prevent access to unauthorised sites,

b) Agree service levels and charging methods with Directors and Heads of Services,

c) Provide regular monitoring information to Directors and Heads of Services to enable them to report any suspected misuse to the Chief Internal Auditor,

d) Provide central administration of email, Internet and intranet services.

e) Make available request forms through the council's intranet and in hard copy,

f) Receive councillors' signed request forms certified by the council's monitoring officer,

g) Receive officers', authorised agents' and partners' signed request forms following their authorisation by an Executive Director, Assistant Director or Head of Service, and

h) Operate a system to enable users to be added to or removed from the council's email, Internet and intranet services.

9.2 Executive Directors, Assistant Directors and Heads of Service

1 The council's Executive Directors shall be responsible for their directorates' use of email and Internet services, and shall;

a) Decide whether officers, authorised agents and partners should have access to email, internet and Intranet services,

b) Manage officers' use of email and Internet services.

c) Inform the council's Chief Internal Auditor of any apparent breach of this policy,

d) Deal with breaches of the policy occurring within their directorate in consultation with the council's Chief Internal Auditor,

e) Inform the Assistant Director responsible for information technology, through the ISS customer service desk, where users have left the council's employment or ceased to be Walsall councillors, and

f) Inform the council's Assistant Director responsible for information technology of any changes in information concerning users. This will include amendment to a user's employment (change of name, job title, service or directorate) affecting their email, Internet or intranet usage.

9.3 Chief Internal Auditor

1 The council's Chief Internal Auditor shall;

a) Alert the council's Assistant Director responsible for information technology and executive directors of any concerns regarding email or Internet use which are discovered as part of the auditing function,

b) Investigate any irregularities reported to them with regard to the usage of email, Internet and intranet services,

c) Inform the police where there are grounds to suspect illegal misuse of the council's email and Internet and intranet systems, and

d) Liaise with the council's Monitoring Officer as appropriate and wherever Councillors are involved.

9.4 Head of Human Resources and Development

1 The council's Head of Human Resources and Development shall:

a) Assist the Chief Internal Auditor by providing information sought in relation to the investigating of any irregularities in the usage of email, Internet and intranet services, including supporting disciplinary procedures,

b) Provide and verify information required by the Head of IT relating to the identity and employment of users and potential users of the council's email and Internet services.

9.5 Councillors, council officers, authorised agents and partners

1 Councillors, council officers, authorised agents and partners shall be responsible for:

a) Complying with the requirements of this policy,

b) Reporting any non-compliance with this policy to the Chief Internal Auditor, and

c) Seeking advice as appropriate.

9.6 Head of Public Protection

1 The council's Head of Public Protection responsible for Environmental Health and Consumer Services shall set aside this procedure only to authorise appropriate officers to:

a) Create email and Internet accounts through other service providers, and

b) Purchase a small number of items under an identity other than that of the council.

2 These actions shall be taken only where necessary for the council's legitimate consumer protection or similar business.

9.7 Schools

1 Each school's governing body shall be responsible for control of Internet and Email usage within their school. Governors shall:

a) Determine the levels of access to be given to students, teaching staff and administrative staff,

b) Ensure that either this policy is followed by the council's employees or that some other suitable policy is put in place,

c) Inform the council's Chief Internal Auditor where any serious breach of this or an alternative access policy may have consequences for areas of the council outside their school,

d) Inform the council's chief internal auditor where any serious criminal activity is suspected, and

e) Seek advice from the council's Assistant Director responsible for Information technology where using the council's servers or other centrally provided equipment.

2 If a school misuses the council's servers or other centrally provided equipment or services, Assistant Director responsible for Information technology may withdraw those services.

Appendix B

Email and Internet policy implementation plan

No	Action	Deliverable	Resource	Start when	Finish When
1.1	Approve Policy	Email and Internet Policy is approved by SLT	SLT, Employee Relations Forum	15/03/07	15/03/07
1.2		Policy approved	Employee Relations Forum	15/03/07	15/03/07
1.3		Final approval	Standards Committee	26/03/07	26/03/07
2.1.	ICT Services to support Policy	E forms created to support revised policy	ISS Development team	01/03/07	31/03/07
2.2.		Electronic signature process to be agreed	Internal Audit, Strategic Transformation team	15/03/07	15/04/07
2.3		Communications plan agreed and implemented	Transformation Communications Editorial board	01/04/07	31/04/07
2.4		Completion of E Form for revised policy	All staff with access to internet and intranet	31/04/07	31/06/07
2.5		Email toolkit and E Learning toolkit amended to incorporate new policy	ISS E learning team and Strategic Transformation Web team	15/03/07	31/04/07
3.0	Monitoring of Policy	Any disciplinary actions that concern email and internet use are recorded and resources involved in the process identified and measured.	Internal Audit Service, HR, Strategic Transformation Team	01/04/07	31/03/08
3.1	Review of policy	Mid year review of policy	Internal Audit Service, Strategic Transformation, HRD	01/10/07	31/10/07
3.2		End of Year Review of Policy	Internal Audit Service, Strategic Transformation, HRD	01/03/08	31/03/08

Appendix C

Risk Assessment

Summary of Risk: **Non Implementation of New Email and Internet usage Policy**

Date of Assessment: **9 March 2007**

IDENTIFYING THE RISK					
Ref	**Risk (ie: Threat to the organisation)**	**Consequence**	**Assessment of Risk**		
			I 1 - 4	**L 1 - 6**	**PR IxL**
	1. That significant officer time / resource is taken up in attempting to clarify omissions / inconsistencies in original procedure. 2. Inability to successfully undertake disciplinary action as a result of alleged misuse of procedure, due to omissions / inconsistencies in original procedure. 3. Users being unaware of council's expectations of them in relation to the council's email and internet, leading to inaccurate / inconsistent application of the procedure. 4. Latest ICT developments are not incorporated in the procedure.	1. Officer time • Additional costs to the organisation providing clarification/ investigation of email/internet use. • Opportunity cost preventing other areas of work not being promptly completed – some of which may be of a higher risk. 2. Unsuccessful disciplinary action • That considerable management and HR resource is engaged on this line of enquiry to the detriment of other case work and/or policy development at a time when the HR service is being reorganised. • That other issues are not progressed. • That significant numbers of colleagues have disciplinary sanctions applied. • Reputation of the organisation as one that is rife with "…." • Potential for costly employment tribunal claims. 3. Unaware of Council's expectations in relation to procedure • Misuse may go un-noticed, and corrective action not taken/ not taken promptly enough. 4. Unawareness of ICT developments • The council's expectations in relation to user's use of the latest ICT developments, such as blogging for example, are unclear; leading to lack of clarity for managers in how to manage such user's actions in relation to these areas.	3 3 3 3	4 4 4 4	12 12 12 12

TYPE: SERVICE DIRECTORATE CORPORATE TEAM PROJECT PLAN

Appendix C

Rating Scores: Impact Catastrophic = 4 Critical = 3 Marginal = 2 Negligible = 1
Likelihood Very High = 6 High = 5 Significant = 4 Low = 3 Very Low = 2 Almost impossible = 1