



Northern Ireland
Assembly

POLICY FOR THE USE OF IT RESOURCES BY NORTHERN IRELAND ASSEMBLY SECRETARIAT STAFF

Issued by: Information Systems Office

Last updated: May 2014

Version Information

Version Number	Author	Date	Comments
1.0	Brendan O'Neill		
1.1	Brian Devlin	August 2012	Revisions to "email guidance" following report of Interim Commissioner for Standards
1.2	Brian Devlin	May 2014	Minor amendments to "Monitoring under Approved and Controlled Conditions"

TABLE OF CONTENTS

Version Information.....	2
INTRODUCTION	4
THE POLICY.....	4
Policy Aims	4
Policy Statement.....	4
Policy Scope	4
Policy Status	4
Policy Application	5
Policy Implementation	5
Policy Responsibilities.....	6
Policy Review and Amendment	7
GUIDANCE ON THE USE OF NI ASSEMBLY IT RESOURCES.....	8
Overview.....	8
General Use of IT Resources - what you need to know:.....	8
Use of Computer Equipment and Software.....	10
What you need to know:	10
Use of Assembly e-Mail Services	11
What you need to know:	11
Use of Assembly Internet Resources	13
What you need to know:	13
Breaches in the Use of IT Resources Policy.....	14
POLICY DEFINITIONS	16
Assembly Information Technology (IT) Resources.....	16
Inappropriate Material	16
Occasional and Reasonable Personal Use.....	17
Routine Logging.....	17
System Logs.....	17
Monitoring under Approved and Controlled Conditions	18
Unauthorised Use.....	18
USEFUL CONTACTS.....	20

INTRODUCTION

1. This Policy and the accompanying guidance detail the acceptable use of the Information Technology (IT) resources provided to Assembly Secretariat staff. The document is divided into three sections:
 - The Policy
 - Guidance on the acceptable use of Assembly IT resources
 - Definitions used in the policy. Any terms for which there are specific definitions have been highlighted in italics at their first occurrence in both the policy and the guidelines.

THE POLICY

Policy Aims

2. The policy aims to ensure that Assembly *Information Technology (IT) resources* supplied by the Northern Ireland Assembly Commission are properly used by Assembly Secretariat staff for the benefit of Assembly business.
3. The application of the policy and its associated guidelines will help to protect the Assembly's IT resources from misuse and ensure the availability and integrity of Assembly information held electronically. It will also protect authorised users from misguided or ill-informed access to, or processing or storage of, information that may be inappropriate or illegal.

Policy Statement

4. IT resources provided by the Northern Ireland Assembly Commission are for use on Assembly business. Additionally, some limited use for private purposes is allowed within the guidance that accompanies this policy.
5. Use of Assembly IT resources for the communication, display or broadcasting of information, images or sound that could cause offence or adversely impact the neutral and harmonious working environment is strictly forbidden. This includes the storage or transmission of *Inappropriate Material* as it is defined for the purposes of this policy.

Policy Scope

6. This policy applies to any Secretariat staff using Assembly IT resources from any location, including any contract or temporary staff employed to do work on behalf of the Assembly Commission.

Policy Status

7. This policy, which comes into force immediately, supersedes the draft 'Code of Practice for the Use of Assembly Computer Resources' which was considered by the Assembly Commission in June 2002. The main change introduced by this policy and accompanying

guidance is to allow limited use of IT resources for ***occasional and reasonable personal use*** and to introduce new countermeasures needed to address increased risks to the security of information held and processed on IT systems.

8. Since the introduction of the Freedom of Information Act 2000 in January 2005 all information held by the Assembly may be subject to disclosure. This includes information generated by or held on computer in any form – including business and personal e-mail and the IT network system logs that record all activity of Internet access. Information recorded by persons acting for the Assembly Commission on the Internet or in an e-mail could be taken as representing the official opinion of the Assembly Commission. Everyone should therefore take particular care when participating in electronic communications using any Assembly IT resource.
9. The Assembly Commission has systems and procedures in place which perform ***routine logging*** of the use of Assembly IT resources. It also holds ***system logs*** which are capable of recording (for each and every user) each Internet site visit, e-mail message and file transfer into and out of the Assembly network.
10. With respect to information held on Assembly IT resources, the Assembly Commission has the right to ***monitor under approved and controlled conditions***. In accordance with the Information Commissioner's Data Protection Employment Practices Code, an impact assessment has been undertaken to clearly identify the purposes behind monitoring and identify any potential adverse impact of monitoring. The assessment concluded that the monitoring of IT systems is necessary to ensure efficient operation of the Assembly's IT investment. Wherever practical, automated systems are used to protect confidentiality; where this is not possible, access is restricted to a limited number of staff who have been educated in the need for confidentiality.
11. The policy has been prepared with consideration of Section 75 of the Northern Ireland Act 1998 and the Human Rights Act 1998.

Policy Application

12. A detailed description of what users should and should not do when using Assembly IT resources is set out in the attached document entitled '**GUIDANCE ON THE USE OF NI ASSEMBLY IT RESOURCES**'.
13. This policy and the guidance will be subject to regular review and revision. Users of Assembly IT resources must ensure that they understand and comply with the policy and guidance.
14. The consequences of not complying with the policy could lead to:
 - legal action against the user and/or the Assembly Commission;
 - reduction of facilities (e.g. removal of Internet access);
 - removal of computer services and equipment; and/or
 - disciplinary action.

Policy Implementation

15. The policy will be implemented through a range of measures which include:

- Awareness guidance for new and existing Assembly computer users on the acceptable use of computer resources; ongoing guidance and advice;
- The continued development and implementation of IT security facilities to protect the Assembly network and Assembly computer users;
- Monitoring under controlled and approved conditions as defined by this policy; and
- Feedback on the effectiveness of this policy – from the IS Office, HR Office, IT User Group and others.

Policy Responsibilities

16. **The Assembly Commission** is responsible for overseeing the policy for the use of Assembly IT resources. It will be informed of misuse of IT resources on (at least) an annual basis.
17. **The Clerk to the Assembly** is responsible for implementing the policy on behalf of the Assembly Commission.
18. **The Director of Resources** will take lead responsibility for the development of the policy and be advised appropriately by the **Head of HR** and the **Director of Legal Services**.
19. **The Information Systems (IS) Office** will continue to apply agreed hardware and software security measures, as approved by or on behalf of the Assembly Commission, to ensure the protection of Assembly IT resources and Assembly staff. IS Office staff may also assist the HR Office in investigations into any breach of this policy.
20. **The HR Office** will make available a copy of the policy for the use of IT resources and the detailed policy guidance for every IT resource user in the Assembly. It will administer any disciplinary procedures which result from misuse of the policy by Assembly Secretariat staff, will publish information on the consequences on the misuse of IT resources and will regularly remind all staff of these consequences.
21. **Line managers** will take appropriate steps to ensure compliance with the policy. They will report any breaches of policy to the Assembly HR Office.
22. **All Assembly IT resource users** are responsible for the proper use of IT resources and complying with this policy. It is the responsibility of everyone to ensure the security of Assembly IT systems at all times. If anyone does not understand any aspect of the policy or guidance they should consult their line manager.
23. Any breach, or suspected breach, of the policy must be reported to the Director of Resources and -
 - For Assembly Secretariat staff – the appropriate line manager, who in turn should inform the Head of HR; or
 - For contract/temporary staff – the Director managing the individual/company.
24. It is a condition of service that all staff comply with this Use of IT Resources policy. Failure to do so will be regarded as misconduct and may result in disciplinary action, up to and including dismissal.

Policy Review and Amendment

25. The Assembly HR Office, in conjunction with the IS Office, will monitor this policy on a regular basis to ensure compliance and to incorporate any major changes that need to be made.
26. The Assembly Commission will review and approve any major changes to this policy.
27. Trade union will be consulted on any changes to this policy.

GUIDANCE ON THE USE OF NI ASSEMBLY IT RESOURCES

Overview

28. This guidance details proper use of the **IT resources** supplied by the Northern Ireland Assembly Commission. It should be read in conjunction with the **Policy for the Use of IT Resources** document.
29. The Assembly Commission provides access to IT resources– PCs, printers, software, e-mail and the Internet – in Parliament Buildings and via remote connection to the Assembly network. The Assembly Commission expects you at all times to use these resources honestly and appropriately. All existing Assembly policies about personal conduct apply equally when using IT resources.
30. IT resources should be used for work-related purposes - i.e. to facilitate business communication with colleagues, research relevant topics and obtain useful work related information. There is also limited scope for ***occasional and reasonable personal use*** of Assembly IT resources, provided that you follow the guidance given in this document. Note that personal use can be withdrawn at any time.
31. All information processed or stored on IT systems, the Internet or in an e-mail could be taken as representing the Assembly Commission's official line and may be subject to disclosure under the Freedom of Information Act 2000. You should therefore have no expectation of privacy when using Assembly IT resources. Unlawful use of IT resources may lead to negative publicity for the Assembly and may expose the Assembly and the individual concerned to significant legal liabilities.

General Use of IT Resources - what you need to know:

32. You are accountable for all activities on Assembly IT resources carried out under your name.
33. The Assembly Commission has the right to ***monitor system logs*** at any time and inspect any and all files stored in any areas of its network or on the hard disk of any of its machines in order to assure compliance with its policies. The right to inspect any information will be exercised under ***approved and controlled conditions***.
34. This monitoring includes access to read any communications made or received by an employee using Assembly IT resources without prior notice for the following purposes:
 - To investigate or detect ***unauthorised use*** of Assembly systems;
 - To intercept for operational purposes, such as protecting against viruses and forwarding e-mails to correct destinations;
 - To check the e-mail system when staff are on holiday or on sick leave; and
 - To investigate problems in the correct operation of computer hardware, software or communication systems.

35. Monitoring does not differentiate between official and personal use, so be aware that each transaction you make - whether by e-mail, Internet or otherwise - is recorded and may be monitored. All communications and information stored on the Assembly's IT resources should not be considered as private. The Assembly Commission may bypass a password you set for monitoring purposes as stated above.
36. The Assembly Commission will take whatever steps it considers appropriate to detect and/or prevent misuse of IT resources. This will include:
- Use of user IDs and/or passwords to maintain individual accountability for computer, Internet and e-mail usage;
 - Installation of Internet firewalls or other security facilities to ensure the safety of the Assembly network and prevent virus infection;
 - Use of industry standard software to identify inappropriate sites and bar access to them;
 - Prevention of connection to the Internet of certain computers holding sensitive data or applications;
 - Blocking of Internet sites which the Assembly regards as inappropriate; and
 - Deployment of systems to identify and prioritise network traffic.
37. The Information Systems (IS) Office will inform users if access to their network account has been granted to others. Access by others will only be given following a signed request from the relevant Director or higher grade. An individual given access to another's account should be aware of their individual responsibilities under the Data Protection Act 1998. Where monitoring is to investigate or detect unauthorised or improper use of Assembly systems by a user, the IS Office must receive a document signed by the Head of HR and the Director (or higher grade) responsible for the management of the user.
38. Please note that the IS Office will never ask for passwords by telephone. IS Office staff will always clearly identify themselves. If you are in any doubt about the validity of a call, take the caller's name and check back with the IT Helpdesk on (028 905) 21000.
39. Unless expressly identified and recorded for a business need (e.g. in connection with a research document) the deliberate access or display of ***inappropriate material*** on any Assembly IT resource, or the transmission of such material to other people, will be treated as a disciplinary offence, or if appropriate as a violation of the Assembly's policy on Harassment and Bullying. This type of material must not be accessed, archived, stored, distributed, edited or recorded using the Assembly's IT resources.
40. You therefore must not create, download, store or distribute any inappropriate material. Specifically, you must not access or transmit any inappropriate material with a sexual content.

Use of Computer Equipment and Software

What you need to know:

41. All computer equipment and software supplied by the Assembly Commission remains the property of the Assembly at all times.

When using Assembly computer equipment and software you must:

42. Comply with all guidelines provided by the Assembly regarding computer use.
43. Keep all user IDs and passwords confidential, as you are responsible for all activities recorded under them. User passwords help maintain individual accountability for Internet use and provide protection for individuals against fraud and misuse.
44. Be alert to the risk of leaving an unattended machine logged on, which could lead to unauthorised use of your account by another person.

When using Assembly computer equipment and software you must not:

45. Connect any equipment to the NI Assembly network without prior permission from the Director of Resources.
46. Install any software, either bought or downloaded from the Internet, without prior written approval from the Director of Resources. Secretariat staff must not purchase any software without approval from the Director of Resources. The IS Office will only provide limited support for non-standard software.
47. Install any screen savers other than those supplied with Assembly machines.
48. Move any computer equipment without permission and assistance from the IS Office. (This includes desktop printers, which can leak indelible ink.)
49. Remove any Assembly-supplied computer equipment from Parliament Buildings without permission from the IS Office. The IS Office will keep a register of those who are authorised to use portable computers for business purposes.
50. Access, modify or interfere with system information held on computer equipment or storage media (floppy disks, CD ROMs, DVD ROMs, tapes etc) belonging to the Assembly without the permission of the Director of Research & Information.
51. Download any virus or program designed to infiltrate the Assembly's computer network to gather information (e.g. worm, Trojan horse). Attempt to disable, defeat or circumvent any Assembly security facility.
52. Attempt to obtain the details (username or password) of any other person. It is an offence for a person to cause a computer to perform any function with intent to secure access to any program or data held in any computer, when the access he or she intends to secure is unauthorised, and when she or he knows at the time that this is the case.

Use of Assembly e-Mail Services

What you need to know:

53. A condition of using the Assembly's e-mail facility is that you accept that the content of all e-mails (personal as well as business) may be accessed under ***approved and controlled conditions*** by authorised staff, without notice or any requirement for further consent. Whilst it is not the policy of the Assembly to undertake routine ***monitoring*** of the content of e-mails, e-mail traffic may be accessed at any time either as a result of checking an officer's e-mail account for business reasons if he/she is absent from work, or to monitor compliance with the use of IT resources or other policies. You should therefore not expect e-mail to be treated as confidential or private.
54. E-mails held on the Assembly network form part of the corporate record of the organisation and are subject to the Assembly's record management policies and procedures. They may also have to be released under the Freedom of Information Act 2000.
55. The Data Protection Act 1998 provides a safeguard for the privacy of some types of personal data. It applies to electronic and paper based personal information and data, including e-mail.

When using e-mail in the Assembly you must:

56. Comply with the Assembly Secretariat's guidance on Assembly correspondence and give care and consideration to the content of e-mail messages, applying similar standards to e-mail as you would to other carriers of information such as fax, telephone and post.
57. Ensure that an e-mail sent to you in error is properly re-directed or returned to the originator. Any e-mail received in the Assembly which is not clearly addressed may be examined by the IS Office to assist in forwarding it to the correct recipient.
58. Take action if you receive what you consider to be an ***inappropriate*** e-mail. You should forward a brief note to the sender informing him/her that you don't wish to receive any further e-mails of that nature and advise your line manager as a safeguard in the event of any subsequent investigation. You should also notify the IS Office.
59. Use the Out of Office Assistant within Microsoft Outlook to inform customers and colleagues when you are unavailable. If you are going to be absent, you should allow a colleague access to read your mail-box so that your e-mails can be monitored and dealt with in your absence. This is particularly important in light of the Freedom of Information Act 2000.
60. Regularly delete any e-mails which are no longer required – from either your inbox, sent or deleted items folders or from any archive folders. If you are in doubt as to whether any information should be retained as part of the corporate record contact the Information Standards Officer on (028 905) 21147.

When using e-mail in the Assembly you may:

61. Make occasional use of the Assembly e-mail system to send brief personal e-mails, subject to the conditions for using e-mail set out in this policy.

When using e-mail in the Assembly you must not:

62. Send any documents which you or others may consider to be private, or disclose official information without proper authority. E-mails are “discoverable” documents in the eyes of the law.
63. Send or store any ***inappropriate material*** in e-mails. If you receive any such inappropriate material via e-mail, you must report the incident to your line manager immediately.
64. Send or publish any information that might be considered defamatory. This includes negative comments about an individual or organisation where the comments may not be accurate.
65. Be any more personal or indiscreet in an e-mail than you would be in a letter or fax which may be read by others than the intended recipient.
66. Attempt to impersonate others, or forge messages or e-mail addresses, or amend messages received by changing the names, dates, times etc.
67. Respond to an inappropriate e-mail from outside the Assembly – spam (unwanted and unsolicited e-mails sent to multiple e-mail addresses), junk-mail or other. Instead you should notify the IS Office. Junk mail is un-requested mail advertising goods or services, jokes and video clips or unsolicited advertisements.
68. Use e-mail to deliberately propagate any virus, worm, Trojan horse, trap door program code or similar malicious program.
69. Promote or participate in ‘chain letters’ by e-mail, which request the receiver to forward the e-mail on to several others. You should delete any such mail immediately upon receipt.
70. Use official templates (e.g. those displaying the Assembly logo) when writing personal e-mails.
71. Send or forward any confidential or sensitive information or documents to a personal email account. (Should staff be required to work at home, remote access to the Assembly network should be arranged. Contact IS Office on ext 21000)

Use of Assembly Internet Resources

What you need to know:

- 72. The Assembly Commission has systems in place that can monitor and record all Internet usage on machines connected to its network, and can examine logs on stand alone PCs which it supplies. These systems can record each Internet site visit, e-mail message and file transfer in and out of the network.
- 73. The Assembly Commission has the right to monitor and record Internet and e-mail usage at any time and inspect any and all files stored in any areas of its network under ***approved and controlled conditions***, in order to assure compliance with its policies, system management and problem solving. This monitoring does not differentiate between official and personal use, therefore if you use the Internet for personal use be aware that each site you visit is recorded and may be monitored.
- 74. The Assembly Commission may block access to any Internet sites which it regards as inappropriate or which may contain inappropriate material.
- 75. Internet usage statistics may be collected and used to analyse usage patterns.

When using Assembly Internet resources you must:

- 76. Give due regard to maintaining the integrity of the Assembly's corporate image and avoid making any references that may prove inappropriate from an Assembly perspective.

When using Assembly Internet resources you may:

- 77. Use NI Assembly Internet facilities for ***occasional and reasonable personal use***.
- 78. This use may include occasional use, at your own risk, of the Internet for online banking or the purchase of goods and services, for example books, flights, etc., provided payment is made by the individual, delivery of items purchased is to a private address and you order the goods using a personal e-mail address. In doing so you must not create any contractual liability on behalf of the Assembly Commission.
- 79. The Assembly does not accept –
 - Any responsibility for the security of credit card details or any other payment method used; or
 - Any liability for losses or other liabilities, howsoever caused, arising from use of Assembly systems for personal transactions. All such use is entirely at the individual's own risk.

When using Assembly Internet resources you must not:

- 80. Deliberately visit, view or download material from any website containing inappropriate material. If you are unsure, do not do it. If you accidentally connect to such a site, you should disconnect from it immediately and report it to your line manager and the IS Office as a safeguard in the event of a subsequent investigation.

81. Download software from the Internet onto the Assembly network, your PC or floppy disk/CD without prior written permission from the Director of Resources. Any such files or software may only be used in ways which are consistent with their licenses or copyright. Any software or files downloaded via the Internet onto the Assembly network becomes the property of the Assembly Commission.
82. Breach copyright rules by downloading, copying or transmitting the works of others to a third party. Copyright is most likely to be breached when downloading material from the Internet, copying text or attaching it to e-mail, using scanned images, browsing music/video or creating/burning CDs. If you are unsure whether copyright will be breached, do not copy! Further advice on copyright can be obtained from the Information Standards Officer.
83. Knowingly allow someone else to use your network account to access the Internet. You are accountable for all activities on the system carried out under your account name. If you suspect that your network account has been compromised in any way, contact the IS Office for advice as soon as possible.
84. Subscribe to any chat rooms, bulletin boards, newsgroups or other Internet services without prior permission from a Director (or higher grade). If you are given permission to use chat rooms etc, do not post any information that could bring the Assembly into disrepute. The Assembly Commission retains the copyright on any material posted onto the Internet by any employee in the course of their duties.
85. Use the Internet to obtain software for personal use – screen savers, games, music, video etc., including playing games on the Internet.
86. Use the Internet to carry out any business or commercial activity – e.g. share dealing or monitoring, investment portfolio management.
87. Use the Internet to deliberately propagate any virus, worm, Trojan horse, trap door program code or similar malicious program; or to disable or overload any computer system or network; or to circumvent any system intended to protect the privacy or security of another user.

Breaches in the Use of IT Resources Policy

88. Management must report any breach, or suspected breach, of the Use of IT Resources policy to the relevant Director.
89. The circumstances will be investigated initially by line management and cases will be subject to normal disciplinary procedures. A breach of the policy may be regarded as a disciplinary matter and a deliberate breach of the policy may be regarded as gross misconduct.
90. The following are some examples of what will be regarded as a breach of the policy and subject to disciplinary action. The list is not exhaustive but is representative of areas or issues that staff should be particularly vigilant about:
 - Impersonating others via e-mail;

- Inappropriate sites visited and line manager not informed;
 - Sending messages which are abusive, offensive, libellous or a nuisance;
 - Disseminating or printing copyright material in violation of copyright laws;
 - Connection of equipment to, or installation of software on, the Assembly network without prior permission; and
 - Over-use of e-mail or the Internet for personal use.
91. In some circumstances, misuse of IT resources may constitute not only a disciplinary matter but also a criminal offence – for example, the possession of child pornography is a criminal offence. The Assembly Commission will co-operate fully with law enforcement authorities to identify and take action against any member of staff accessing, possessing or disseminating such material. Individuals found to have been involved in any way in the possession or dissemination of child pornography using Assembly systems will face disciplinary action.
92. You should note that you might be personally liable to prosecution and open to claims for damages should your actions be found to be in breach of the law. In cases of harassment, a claim that you had not intended to harass or cause offence may not in itself constitute an acceptable defence.
93. Unless expressly identified for a business need, the use of IT resources to disseminate inappropriate material which could cause offence to others (irrespective of whether any offence is intended) may constitute harassment and will not be tolerated. The business need must be justified in writing by the Director of the relevant business area.

POLICY DEFINITIONS

94. The following is a list of the main definitions used throughout the policy.

Assembly Information Technology (IT) Resources

95. Assembly IT resources as referred to in this policy is defined as:

- Computing equipment such as PCs, portable computers, printers or other computer hardware supplied by the Assembly Commission for business purposes;
- The Assembly network, including access to the World Wide Web (Internet), either remotely or from within Parliament Buildings; and
- Computer software supplied by the Assembly Commission and installed on equipment provided or funded by the Assembly Commission, including e-mail facilities.

Inappropriate Material

96. The following is considered to be inappropriate material for the purposes of this policy:

- Material which is sexually explicit, obscene, pornographic or indecent, whether messages, images, jokes or cartoons;
- Material which is defamatory, offensive, harassing or threatening;
- Material which may harass, provoke, demean, degrade, threaten, insult, victimise or discriminate against anyone or a group of people, particularly on grounds of gender, religious belief, sexual orientation, political opinion, racial group, age, marital status, family or part-time status, disability or trade union membership/non-membership;
- Material which includes malicious gossip or inappropriate personal information about others;
- Material which may be of embarrassment to the NI Assembly or the NI Assembly Commission;
- Material which is concerned with the user's commercial enterprise or conflicts with the interests of the Assembly;
- Material which introduces viruses into the Assembly's computer network. The deliberate introduction of a virus is a criminal offence.
- The sending of Internet chain letters which request the receiver to forward the e-mail on to several others;
- The sending, exchange or storage of games and 'junk mail' – e.g. un-requested mail advertising goods or services, jokes and video clips, unsolicited advertisements.

97. This material includes information stored or transmitted on PC, portable computer, floppy disk, CD, DVD or mobile phone - whether photograph, moving image, sound file, graphic or cartoon and whether or not it purports to be of a humorous nature.

Occasional and Reasonable Personal Use

98. The Assembly Commission permits staff to use Assembly IT resources for personal use, in their own time and with the agreement of their line management, providing that such use does not -
- Have an adverse impact upon their availability to carry out their normal work;
 - Compromise the security of Assembly data;
 - Result in increased costs or delays; or
 - Have any negative impact on the Assembly network or on the effective discharge of Assembly business.
99. The facility is granted at the discretion of management and may be withdrawn at any time for operational reasons or if inappropriate use is suspected.

Routine Logging

100. Routine logging of IT resource use is performed to protect Assembly computing facilities from disruption due to security breaches, computer hacking or virus attack. It is also to assist the business in ensuring that IT users receive information in a secure and timely manner, and to ensure that computer systems run efficiently and effectively. Checks undertaken include the following:
- The Assembly examines a summary of websites visited on a daily basis to ensure the correct functioning of network equipment. This does not involve the detailed examination of individual visits to websites; however a more detailed examination may be required to correct problems with a specific machine or user account.
 - The Assembly monitors misdirected e-mails in order to redirect them to the correct individual. This may include examining the contents of the e-mail message to determine the intended recipient. There is no routine examination of the content of e-mails.
 - Automated security systems may block e-mail attachments. The intended recipient is automatically informed that attachments have been blocked and these may be forwarded on request to the IT Helpdesk. To protect the security of computer resources, e-mails which contain attachments potentially associated with viruses will not be forwarded.
 - The Assembly Commission blocks access to Internet sites which would breach this or other Assembly policies or are associated with virus distribution or internet scams.

System Logs

101. System logs are capable of recording (for each and every user) each Internet site visit, e-mail message and file transfer into and out of the Assembly network. System logs are

normally kept for a maximum of 6 months to provide adequate statistics to assist in identifying equipment performance and usage trends. Where possible, monitoring of system logs is automated. However the Assembly Commission has the right to monitor and inspect system logs or communication made or received by an employee using Assembly IT resources without prior notice and under controlled and approved conditions.

Monitoring under Approved and Controlled Conditions

102. Before the monitoring of system logs is undertaken, the IS Office must receive a document giving as much detail as possible on the examination required – e.g. network user name, dates between which information is to be examined, parameters of the examination (whether e-mail, internet or file logs) from the Director (or higher grade) responsible for the business area in which the user is currently working. Approval to proceed with the examination must be signed by the Head of HR and the Director of Resources. During the formal examination of information, at least one member of staff from both IS Office and HR will be present.
103. Monitoring will only be performed for the following purposes:
 - To investigate whether there has been any unauthorised or improper use of Assembly systems;
 - To intercept such material for operational purposes, such as protecting against viruses and forwarding e-mails to correct destinations;
 - To check the e-mail system when staff are on holiday or on sick leave. Staff who are going to be absent should allow a colleague access to read their mail-box so that the e-mails can be monitored and dealt with in their absence; and
 - To investigate problems in the correct operation of computer hardware, software or communication systems.
104. This may involve the examination of any system logs of computer resources used or accessed by any Assembly employee. It may include any Internet access, e-mail communications, e-mail or file content.
105. In accordance with the Information Commissioner's Data Protection Employment Practices Code, an impact assessment has been undertaken regarding the monitoring of information held on Assembly IT resources. This has been undertaken to clearly identify the purposes behind monitoring and identify any potential adverse impact of monitoring. Wherever it is practicable, automated systems have been used to protect confidentiality; where this is not possible, access is restricted to a small number of IS Office staff that have been educated in the need for confidentiality. A copy of the full Impact Assessment is available from the IS Office.

Unauthorised Use

106. Use of Assembly IT resources by a member of Secretariat staff which has not been properly approved is deemed unauthorised use. Unauthorised use may also include use by an authorised user for purposes that are contrary to the policy, for example accessing, displaying or transmitting inappropriate material. Provision of a network account for an individual must be approved by their Head of Branch or higher grade; the work to provide

this will be authorised by the ICT Infrastructure Manager or higher grade within the IS Office. Access to specific systems and information other than that supplied as standard will be provided as a separate request approved by the Head of the Branch which is deemed to control the information.

USEFUL CONTACTS

If you require further information or have any questions on this policy, please contact any of the following:

Director of Resources	(905) 20901
Information Systems (IS) Office	(905) 21000
Head of HR	(905) 24252
Information Standards Officer	(905) 21147