Edinburgh Napier University - Electronic Information Security Policy

Monitoring and Logging Policy

1. Introduction

Edinburgh Napier University's policy is that information it manages shall be protected against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information to authorised users. For information security to be effective it requires the participation and support of all Edinburgh Napier University staff, student and other persons who have access to its information technology.

Information security at the University is governed by its Electronic Information Security Policy which consists of an Overall Policy and a number of subsidiary policies. This subsidiary policy covers the monitoring and logging of all uses of information technology. It is the responsibility of every information technology user to know these policies, and to conduct their activities accordingly.

Additional policies cover specific issues, technologies and types of usage are listed below:

- Overall Policy
- User Policy

Links to the Overall Policy and User Policy can be found in the following locations:

Staff: go to the "IS Policies" page within the Information Services section of the Staff Intranet.
Students: go to the "Information Security Policies" page within the IT section of My Napier.

2. Monitoring

Networks and computers may be monitored, and usage logged. Logs are kept secure and are only available to personnel authorised by the Director of Information Services and will only be kept as long as necessary in line with current data protection guidelines.
Edinburgh Napier University's networks and computer may be monitored and logged for all lawful purposes including: -

- Ensuring use is authorised
- Management of systems
- Protecting against unauthorised access
- Verifying security procedures
- System and operational security
- Compliance with Edinburgh Napier University policies and regulations
- Detection and prevention of crime

Monitoring includes active attacks by authorised Edinburgh Napier University users to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorised purposes. All information, including personal information, placed on or sent over this system may be monitored. Monitoring is automated in the detection and removal of viruses, malware, spam, pornographic and inappropriate URL's and other activities not lawful to University business. Use of the Edinburgh Napier University information technology, authorised or unauthorised, constitutes consent by the user to monitoring of these system. Unauthorised use (as outlined in the Electronic Information Security Policy Statement and associated policies) use may give rise to disciplinary procedures or criminal prosecution. Evidence of unauthorised use collected during monitoring may be used subsequently in a disciplinary, criminal or another form of proceedings. Use of the Edinburgh Napier University IT systems constitutes consent to monitoring for these purposes.

3. Email Scanning

Incoming e-mail may be scanned by Edinburgh Napier University including using virus-checking software. The software may block unsolicited marketing e-mail (spam), e-mail which has potentially inappropriate attachments, bad language or any other inappropriate material. If there is a suspected virus in an e-mail the sender will automatically be notified, and you may receive notice that the e-mail is not going to be delivered to you because it may contain a virus.

4. Law

In accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act (Scotland) Act 2002, the University will exercise its right to intercept and monitor electronic communications received by and sent from the University for the purposes permitted under those Regulations. The purposes cover, but are not limited to, monitoring for criminal or unauthorised use, viruses, threats to the system e.g. hacking and denial of service attacks, ensuring the effectiveness of its operations and compliance with University policies and regulations.

5. Regulations Explained

Regulation of Investigatory Powers Act 2000

As required by UK legislation, all users of the University's Data and Telephones Networks must be aware of the fact that their communications may be intercepted as permitted by legislation.

The legislation allows the University to intercept without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance with University policies, detecting crime or unauthorised use, and ensuring the operation of our systems. The University does not require to gain consent before intercepting for these purposes but needs to inform staff and students that interceptions may take place (see section 4)

In the course of their normal duties some authorised staff have the authority and are required ` to carry out certain monitoring activities in order to ensure the correct operation of telecommunications systems. This does not imply that all communications are monitored, just that they MAY be for the above purposes. The Act is available here:

http://www.opsi.gov.uk/legislation/scotland/acts2000/asp_20000011_en_1

Data Protection Act 1998

Information Services (IT) and other information technology providers in the University, holds user registration data and information on the use of the University's computer systems and network. The information when and where users have logged in or out, printing logs, Internet cache logs, door access control logs, web sites visited, network traffic logging and other similar logging will be logged.

While normally only used for resolving operational problems, these logs will be analysed (under the University's Security Policies) down to the individual user where a breach of the University Regulations and policies or other misuses and abuses of the facilities is suspected.

The information extracted from logs referred to above will also be used to communicate with individuals to alert them to malfunctions within Edinburgh Napier University IT facilities or to request action to correct the malfunctions which may be putting the normal operation of the IT facilities in jeopardy.

In addition, statistical analysis may take place, which does not identify any individual, to provide management information on computer lab, door access, software, printing, cache, network and general computer usage. For further information check the Data Protection Intranet pages: http://staff.napier.ac.uk/services/secretary/governance/DataProtection/CodeofPractice/Pages/default.aspx

Or contact the senior responsible officer for Data Protection for Edinburgh Napier University.

The Data Protection Act 1998 is available here:

http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1