# Edinburgh Napier University - Electronic Information Security Policy

## User 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 which can be found in the 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.

This subsidiary policy covers everything that an information technology 'user' requires to know. 'Users' are those that only use services provided to them as part of their role at the University and in the way the services are intended to be used by the service provider. It is the responsibility of every information technology user to know these policies, and to conduct their activities accordingly.

The purpose of this policy is to state clearly the users' obligations in using Edinburgh Napier University information technology responsibly, professionally, ethically and lawfully. Additional policies cover specific issues, technologies and types of usage.

## 2. Scope

The Electronic Information Security Policy applies to all staff and students at the University and any other persons who are authorised to access the University's information technology facilities.

This policy covers all uses of information technology. Specifically, this policy applies to all use of information technology on the University's premises even if the University does not own the equipment, to all information technology provided by the University wherever it is used, and to all external access to the University's information technology from wherever this is initiated.

**N.B.** The above scope covers all University related working from home.

## 3. Enforcement

Failure of a user to comply with any part of the Electronic Information Security Policy will lead to the relevant disciplinary procedures being invoked. In certain circumstances actions may be reported to the police or legal action may be taken.

## 4. Monitoring & Logging

Edinburgh Napier University will monitor network activity. Information Services will proactively consider reports from JANET Computing Emergency Response Team (JANET CERT) and other security sources and take action and/or make recommendations that maintain the security of Edinburgh Napier University's Information Security.

For full details on monitoring please refer to the **Monitoring and Logging Policy** which can be found in the 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.

## 5. Use of Systems and Information

Edinburgh Napier University's information technology is provided to support educational and business functions of the University including access for personal development to improve individual knowledge, skills and career enhancement. The only other usage allowed is as defined in section 6 under 'personal private use of information technology'.

Information must NOT be offensive, abusive, discriminatory, illegal to possess, damage the University's interests, or contravene University regulations. Examples of offensive information include all forms of pornography and violent images. Pornography as defined here includes:-

i) Indecent images of children under 18 which it is illegal to possess.
ii) Obscene materials which it may be an offence to publish but not to possess.
iii) Materials comparable to that available on the "top shelf" in a Newsagent which is neither an offence to publish nor possess but which some may find distasteful.

This section applies equally to all storage, processing or transmission of information, examples including viewing of web pages, data files and the content of emails.

It is acknowledged that there can be valid academic reasons to access information that would normally not be allowed under this policy. In this situation staff and students must gain written approval from their Dean of School or Director of Service for these specific activities. Information that it is illegal to possess is never allowed.

The University recognises that users may accidentally connect to unacceptable web sites or receive unsolicited unacceptable emails. Audit logs will demonstrate that such visits are rare and short, and hence unintentional. In these cases, no action will be taken against the user.

Users must only attempt to access information technology services which are either clearly publicly available, for example public web sites, or ones to which they have been personally granted specific rights by the administrator of that service.

If a user is not sure whether they have rights to access a service, they must contact the manager of that service before attempting access.

No forms of 'network probing or sniffing' are permitted unless specifically approved in writing by the Director of Information Services, as advised by the senior responsible officer for Information Security, who can be contacted via the IS Service Desk. A breach of this part of the policy is normally a criminal offence as it constitutes illegal use of hardware, software or information.

The University has a statutory duty 'to have due regard to the need to prevent people from being drawn into terrorism'. The use of IT facilities to support terrorist activity is not permitted and may result in a criminal charge. Access to material promoting terrorism is not permitted, unless this access has been specifically allowed by the University Ethics Committee as part of an approved programme of research.

## 6. Personal Private Use of Information Technology

Edinburgh Napier University allows personal/private use of its information technology by staff and students subject to the following conditions.

i. It must not inconvenience or distract any educational or business function.
ii. It must not in any way interfere with their individual work as a member of staff or a student at the University.
iii. It must not in any way impede the work of other users.
iv. It must not place a heavy load on the systems. (Examples of types of use that are not allowed include the transfer of music and video files, the playing of games over the network, or similar network intensive activities.)
v. Any personal financial transactions conducted using University IT facilities are done at the individual's own risk.
vi. Private use specifically excludes private commercial activity, betting and gambling.

Personal private use may be withdrawn on an individual or group basis if it is abused or interferes with the efficient operation of the University.

## 7. Passwords

This section defines the regulations for the use of passwords that are critical as they are the 'keys' to all information technology security.

1. All workstations must be protected with a password. (This function is carried out by Information Services for workstations on the University network)

2. Authorised users are responsible for the security of their passwords and user accounts. Passwords must be kept secure and never shared with anyone else.

3. Passwords must be at least 7 characters long and include alpha, numeric and at least one other character. Their structure must make them hard to guess. Guidance on creating passwords is available on the University Intranet:

   **Staff:** go to the "Cyber Security" pages within the Information Services (IT) section of the Staff Intranet.
   **Students:** go to the "Staying Safe Online" page within the IT section of My Napier.

4. Passwords should never be displayed on screens.

5. If at anytime a user thinks someone may have discovered their password, they must immediately change it or request that it is changed.

6. At times, normally when the user has forgotten their password, it will be necessary for passwords to be changed by system operations. In these cases, proof of identity will be required as for account/password creation.

7. Passwords should never be “remembered” on the computer but entered by the user on all occasions.

## 8 General Acceptable Use

This section defines general regulations that govern the use of information technology: -

1. Always log off or lock a workstation before leaving it. This is to ensure that no one else can access the user’s information or has the opportunity to use the workstation without identifying themselves, e.g. to send an abusive email in the user’s name.

2. When confidential work is being carried out ensure no one else can read the screen.

3. Protect equipment from physical theft, this is vitally important for portable equipment.

4. Ensure that all important data is backed up regularly and copies kept in a separate secure location. Liaise with the IS Service Desk if you require assistance. (This function is carried out by Information Services for information stored on the University network).

5. Respect the legal protections for information and software provided under copyright and licenses. Never copy electronic information or computer programmes unless specifically authorised in writing. Never run or install software without a valid licence.

6. Licensed electronic reference information and computer software must not be used for ‘non core’ University purposes without the specific written authority of the Dean of School or Director of Service holding the licence on behalf of the University. For this purpose, such ‘non-core’ activities include consultancy, student projects that benefit other organisations (including their employers) and presenting short courses.

7. Do not move information from the University premises unless it is really necessary. All personal and business critical information moved using data storage devices should be protected using approved encryption software.

8. All PCs should be patched with the latest security critical patches and up to date patches.

9. All data storage devices including laptops, USB sticks, CD’s, DVD’s that are brought into the University must be checked for viruses on every occasion before use.

10. All workstations connected to the Edinburgh Napier University network whether owned by Edinburgh Napier University or not shall be continually executing approved virus-scanning software with a current virus database.

11. Never introduce malicious programs into the Edinburgh Napier network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) by any means.

**N.B.** Points 8 – 11 are carried out on all University workstations running the standard Information Services images.

Physical devices include laptops, iPads, mobile phones, USB sticks, CDs, DVDs etc. and all other mobile devices.

Inform the IS Service Desk immediately if you think that any workstation may have a virus or is behaving abnormally.

## 9. **Email and Internet Use**

This section defines the regulations to ensure secure use of email and the internet.

1. Always check the address line before sending a message and check it is being sent to the correct person (one of the most common forms of alleged security breaches).

2. Never represent yourself as another person or persons.

3. Delete electronic mail messages when they are no longer required.

4. Take care not to express views, which could be regarded by others as offensive or libellous. Comments made in jest may be misinterpreted by the recipient. In a case of harassment, it is the effect of a communication on the recipient that is considered and not the intention of the sender.

5. Any personal private emails must be saved in a separate folder from work related emails. Clearly mark all emails that are of a personal nature as “personal”.

6. Personal/private postings to wikis, blogs, newsgroups or similar referencing Edinburgh Napier University must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Edinburgh Napier University.

7. Users must not open e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code or any other form of Malware.

8. Do not forward electronic mail messages to other individuals or groups that have been sent to you containing personal data (as defined by the Data Protection Act 1998) without the permission of the originator.

9. Do not participate in chain or pyramid messages or similar schemes.

10. Do not unnecessarily send excessively large electronic mail messages or attachments.

11. The University network and the internet connection are not to be used for peer-to-peer file sharing except with the permission of the Director of Information Services.

12. Report any unusual or suspect email messages or network activity to the IS Service Desk.

If there are any questions regarding any of these regulations contact the IS Service Desk by emailing ISServiceDesk@napier.ac.uk or telephoning extension 3000.

## 10. Guidelines

For guidelines on information security check the Edinburgh Napier University intranet pages:

**Staff:** go to the “Cyber Security” pages within the Information Services (IT) section of the Staff Intranet.
**Students:** go to the “Staying Safe Online” page within the IT section of My Napier.