NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

FACULTY OF COMMUNICATION AND INFORMATION SCIENCE

DEPARTMENT OF LIBRARY AND INFORMATION SCIENCE

MASTER OF SCIENCE DEGREE IN LIBRARY AND INFORMATION SCIENCE

STAGE I FIRST SEMESTER NOVEMBER 2012 EXAMINATIONS

ILI 5101: ADVANCED INFORMATION TECHNOLOGY APPLICATIONS

TIME: 3 HOURS PLUS 15 MINUTES READING TIME

Instructions to candidates

1. Answer four (4) questions
2. Question **1 is compulsory**
3. Each question carries 25 marks.
4. Importance is attached to accuracy, clarity of expression and legibility of handwriting.

1.1 Evaluate the attached ICT usage policy for vulnerabilities. [10 marks]

1.2 Indicate the risks associated with the vulnerabilities you have identified. [7 marks]

1.3 Suggest justified amendments to this ICT usage policy, to enable the policy to be relevant to an information centre of your choice. [8 marks]

2. Assess the functions of each of the following layers of the OSI reference model:

2.1.1 Data link layer [4 marks]
2.1.2 Transport layer [4 marks]
2.1.3 Physical Layer [4 marks]

2.2 Examine any three (3) common Application Layer Protocols that are useful in Library information centres. [13 marks]

3.1 Discuss three (3) types of cryptographic algorithms, showing how they impact on digital libraries. [15 marks]

3.2 Outline two (2) other security procedures that may be implemented. [10 marks]

4. Search engine optimisation, RSS feeds and Facebook are some of the effective ways of reaching an electronic audience. Critically evaluate these methods indicating any other two ways of reaching electronic audiences. [25 marks]

5. Discuss the concept of supply chain management with reference to electronic library information systems. [25 marks]

6.1 Discuss critical issues to be taken into consideration when designing the following:

6.1.1 B2B site [4 marks]

6.1.2 B2C site [4 marks]

6.1.3 G2G site [4 marks]

6.2 Assess the impact of EDI and EFTs on library information centres in Zimbabwe. [13 marks]

END OF PAPER

ACADEMIC LIBRARY ICT USAGE POLICY

1. Acceptable Use

Users of this library are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

2. Network Etiquette and Privacy (Internet and Email)

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

• Professional conduct must be maintained at all times.

• Be polite – never send or encourage others to send abusive messages.

Defamatory comments could result in legal action. E-mail has been used successfully as evidence in libel cases.

• Use appropriate language – users should remember that they are representatives of the library on a global public system. Illegal activities of any kind are strictly forbidden.

• Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.

• Do not view, send or retain any offensive or illegal material. This includes any jokes or content such as that contains racist terminology, violence, pornography or any material that might constitute harassment.

• Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users files or folders.

• Password – do not reveal your password to anyone. If you think someone has learned your password then contact the Network Manager. Users are responsible for any misuse recorded under their username.

• Electronic mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities.

• Disruptions – do not use the network in any way that would disrupt use of the network by others.

• Staff or students finding unsuitable websites through the library network should report the web address to the Network Manager as soon as reasonably possible

• Do not introduce portable media devices such as floppy disks, pen drives, into the network without having them checked for viruses.

• Do not attempt to visit websites that might be considered inappropriate. All sites visited leave evidence on the network if not on the computer.

Downloading some material is illegal and the police or other authorities may be called to investigate such use.

3. Chat Rooms

Students will not be allowed to access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them. Chat sites are banned under the library filtering system. Under exceptional circumstances, a chat site could be made available provided the library staff takes precautionary measures • The Chat site is only made available to staff for a specific professional purposes.

4. Forums

Forums that are available to users of the internet need to be moderated to ensure correct use and no offensive posts are made. This means that someone in the library will have to approve every post that is made to the forum.

5. Additional Email protocols

• All users must follow the guidelines set out in the Network etiquette section of this document.
• Staff & Students may only use approved e-mail accounts on the library system. Access in library to external personal e-mail accounts may be blocked. For example - Hotmail is blocked.

6 Unacceptable use

- Examples of unacceptable use include but are not limited to the following:
- Users must login with their own user ID and password and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety.
- Sharing of digital recordings by any device (video, photos or sound). If a student is found to have done this, the library may consider recommending a permanent exclusion. This may also be considered if any technology is used for intimidating behaviour or an attempt to bring the library into disrepute.
- The use of Facebook is prohibited.
- Searching for, looking at, creating or publishing offensive material.
- Failure to adhere to these protocols may result in loss of access to the Internet as well as other disciplinary action.

7. Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the library. The library will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

8. Network security

Users are expected to inform the Network Manager immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

9. Physical security

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms.

10. Wilful damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the library system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

11. Security and Virus Protection

Any malicious attempt to harm or destroy any equipment or data owned by another user will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

12. Network Security

Users are expected to employ good password practice when using the network. This includes keeping personal passwords secure and always logging off after use. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

The Library Network Manager will ensure that:

- The server operating system must be secured to a high level.

- Anti Virus software is both installed throughout the network and kept up to date. This includes taking steps to allow staff laptops to receive updates either at home or within the library.
- Hardware Security measures are adhered to: including ensuring that laptops, digital still and video cameras are securely locked away when they are not being used even during breaks and lunchtimes
- Users identified as a security risk may be denied access to these types of equipment.