fashion&designinstitute

Student Internet Usage Policy Version 1.1

A. Purpose

The purpose of the Student Internet Usage Policy is to ensure that

a) The student of the Fashion and Design Institute (FDI) is informed about the applicability of policies to the use of Internet;

b) The Internet access provided is being used in compliance to those policies

c) Users of Internet are informed about the security risks of the Internet.

B. Scope

The scope of the Internet Usage Policy applies to:-

a) All internet access services provided or owned by the Fashion and Design Institute; and

b) All users, including those from outside the building, who have access to the Internet through Fashion and Design Institute infrastructure.

C. General

1. The Fashion and Design Institute encourages the use of Internet as a learning and study tool. The Fashion and Design Institute of Mauritius retains the copyright to any material posted on the Internet by any student in the course of his or her study.

2. Internet access is provided for education use only.

3. Students should not use Internet facilities of the Fashion and Design Institute for any unlawful purposes nor personal financial gains and should agree to abide by all applicable national laws and regulations. Students with Internet access may not upload to the Internet any software owned by or licensed to the Fashion and Design Institute without the necessary written authorization from the Management of Fashion and Design Institute.

4. The browsing of any kind of offensive materials on any Fashion and Design Institute of computer/network system is strictly prohibited. In addition, such offensive materials may not be archived, stored, distributed, edited or recorded using the network or computing resources of the Fashion and Design Institute.

5. No student may use the Internet facilities of the Fashion and Design Institute of Mauritius to propagate any virus or other malware.

6. No student may use the Internet facilities of the Fashion and Design Institute to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

7. The Fashion and Design Institute reserves the right to block Internet sites as it deems necessary to enforce compliance to this policy.

8. The Fashion and Design Institute of Mauritius reserves the right to monitor all Internet usage and to inspect any or all files stored in private areas of the network in order to assure compliance with policy.

9. Student(s) need to adopt a code of conduct and code of ethics while surfing the Internet (social media, chat service, forums etc.) to assure not to post or behave in any such way which can cause harm or tarnish the goodwill of Fashion and Design Institute toward the public, FDI staff or FDI partners or/and students

D. Guidelines

1. User ID and passwords help maintain individual accountability for Internet resource usage. Any student who obtains a User ID/password for an Internet resource from the Fashion and Design Institute must keep that User ID/password confidential.

2. Individual passwords must never be shared or revealed to anyone. To give a

password to someone exposes the authorized user to responsibility for the actions the other party takes using this password.

3. Students using laptop/computers not belonging to the institute connected to the Fashion and Design Institute WIFI/network access the internet or otherwise should be equipped with the updated version and definitions of anti-malware/antivirus software.

4. Students with Internet access may not use Internet facilities of the Fashion and Design Institute of Mauritius to download entertainment software or games, screensavers or to play games over the Internet.

6. Users should be aware that screensavers and games downloaded over the Internet may contain spyware or viruses. Spyware gathers user information for advertising purposes and monitors user activity on the Internet. All students should be fully aware of and comply with the Internet Usage Policy.

E. Responsibility for Policy

The Fashion and Design Institute Information Technology section is responsible for the development and maintenance of this policy. The responsibility for ensuring compliance with this policy lies with the Information Technology section and Management.

F. Internet Monitoring Procedures

1.1 The Fashion and Design Institute maintains a policy of blocking access to web sites which may include:

a) Sites of non educational use from where heavy downloads are being effected

b) Sites containing pornographic or other material that could be deemed offensive

c) Downloadable files with extensions as at Annex A

1.2 Monitoring is done on a regular basis at the FDI. The report gives an indication

of who has used the most bandwidth. Websites visited and files downloaded are crosschecked. If usage is very high and abusive, a live monitoring is performed on the Proxy server to check which websites are being accessed and what is being downloaded. If websites and downloads are found to be non-education related and abusive, the user IP is blocked and concerned party notified.

1.3 The blocking of offensive sites is automatically made by a control mechanism in place at the FDI. Categories of blocked access are at Annex B.

1.4 However, during monitoring of Internet Usage patterns, the FDI may find it necessary to manually include additional sites deemed offensive in its blocked list at any point in time.

1.5 Accesses to the Internet are logged and monitored on a daily basis at the level of the FDI.

1.6 Students attempting to access a blocked site are automatically notified with a warning sign and the attempt is logged. Repeated attempts will be handled as an abuse and action taken accordingly.

1.7 Downloads exceeding 100 Mb per day from a specific IP Address/User will be blocked.

1.8 There will be immediate blocking of IP addresses where there has been evidence of breach of the Internet policy (e.g. downloads greater than 50 MB).

of Mauritius may carry out investigation which may entail disciplinary or legal action

Annex A – File Extensions Blocked

1. Mp3 – music file
2. Flv – movie file
3. Avi – movie file
4. Mp4 – movie file
5. Wma – music file
6. 3gp – mobile movie file
7. Divx – movie file
8. Xvid – movie file
9. Rmvb – movie and audio for real media player
10. Wmv – movie file
11. Rm – audio for real player
12. Mpg – movie file
13. Exe – executable file
14. Dat – binary data file

Annex B – Categories of Sites Blocked

1. Adult / Sexually Explicit
2. Adverts & Pop-ups
3. Criminal Activity
4. Gambling
5. Games
6. Hacking
7. Illegal Drugs
8. Intolerance & Hate
9. Peer to Peer
10. Phishing & Fraud
11. Proxies & Translators
12. Ringtones/Mobile Phone Downloads
13. SPAM URLS
14. Spyware
15. Streaming Media
16. Tasteless & Offensive
17. Violence
18. Weapons

IT End User Guidelines.

PC Housekeeping

- Smoking in the vicinity of computers must not be allowed. Smoke raises carbon particles, which may enter into the computer and create hazards.
- Eatables and drinks must not be allowed near computers to minimize risk of damaging equipment (e.g. keyboards) by spilling food.
- Back up of your PC data must be done regularly, optical disk (CD/DVD or on other external media. Note that pendrive/flashdrive is not a recommended long life backup measure.
- Use of pirated and unauthorized software should be strictly prohibited as these may contain viruses.
- Only original software purchased from authorized vendors should be used.
- Ensure you have the latest version of antivirus definition and software. The antivirus must be regularly updated and must have its permanent shielding facility on else proper protection means be used to avoid device contamination.

Using E-mail

- Beware of e-mail from unknown parties (unsolicited e-mail). Do not open unsolicited email. Do not take action based on information in unsolicited e-mails e.g. 'You have won $1,000,000. Kindly send your bank details for crediting your account' or Job offers asking for your personal details. These are scams also known as social engineering attacks, which may lead to your personal data manipulation and spoofing or/and financial lost.
- Ensure you are addressing the right person (known and trustworthy) prior to sending e-mail.
- Executable files (e.g. with .exe, .com, .bat, .reg extensions) and suspicious attachments must not be opened.
- Do not subscribe to unnecessary or unverified mailing lists. You may end up receiving an overload of e-mails that may slow down your computer. Such e-mails are known as spam.

Safe Internet Surfing

- Avoid giving unnecessary information online (e.g. Subscribing to a newsletter whereby your family details are requested).
- Do not surf on sites that contain offensive material.
- Do not download software cracks, free software (from untrustworthy sites), games, screensavers and other unnecessary gimmicks from Internet – they may have embedded spyware or viruses. Usually spyware covertly gathers user information for advertising purposes and monitors user activity on the Internet. Spyware can also gather information about e-mail addresses, passwords and even credit card numbers and transmit that information in the background to someone else.

Password Management

Passwords should ALWAYS contain:

- At least eight characters
- Both upper and lower case letters
- At least one number
- At least one special character (for example # $ % {+ ?)
- Passwords should NOT:
- Be based on personal information, such as names of family, dates, addresses, phone numbers, etc.
- Be based on work information, such as room numbers, building name, co-worker's name, phone number, etc.
- Use word or number patterns like, aaabbb, qwerty, zyxwvuts, 123321, abcABC123, etc.
- Hard to guess passwords must be used. A poorly chosen password may result in the compromise of your computer.
- Password should be regularly changed.
- Password should not be shared with anyone

Student Protection

It is our intention to protect students from inappropriate or undesirable material. The following criteria define inappropriate or undesirable materials:

- Obscene, offensive or inaccurate.
- Students must not insult, attack others, violate copyright, trespass in others' folders or harass anybody through the internet.

Under the **Computer Misuse or Cybercrime Act 2003 the Act** provides for a repression of criminal activities perpetuated through computer systems. Attention is drawn to the following:

Indecent or Obscene photographs of children

Any person who –

a) takes or permits to be taken or to make, any indecent photograph or pseudo-
Photograph of a child; or

b) Distributes or shows such indecent photograph or pseudo-photograph; or

c) Has in his possession such indecent photograph or pseudo-photographs, with a view to it being distributed or shown by himself or any other person; or

d) publishes or causes to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photograph or pseudo-photograph, or intends to do so,**shall commit an offence.**

Filters

The lab network system is set up in accordance with appropriate practices for security purpose. The Fashion and Design Institute have Internet access filtering device. This filter screens out materials that are deemed as being unsuitable or undesirable against an automatic white and black listing.

Supervision

During classes in the Computer Lab, the computers can are monitored by the staff present to ensure students are using appropriate web sites.

Note: This policy section may be updated as and when required without prior notice. Latest version of the document should be used. It is the responsibility of the user to keep update with the latest version available

- **IT Section -**
July 2014