

THE INTERNET, WEB 2.0 & OTHER EXTERNALLY HOSTED SERVICES

GUIDANCE FOR STUDENTS: HOW TO BE WEBWISE

INTRODUCTION

The purpose of this guidance is to:

- encourage you to use the internet, Web 2.0 and other externally hosted services (e.g. Facebook, Second Life, Delicious) in a safe, responsible and acceptable way
- protect you from electronic abuse or harassment by a fellow student and/or others
- make you aware of the relevant legal issues; and
- protect the reputation of the University

SUMMARY

This guidance applies to all internet presence, including participation in online communities and hosted services (e.g. social networking sites, forums and public messaging services) and maintaining personal profiles or pages (e.g. blogs) by which personal information or opinions can be uploaded for public consumption. The key points which you need to know about are:

- **Data Protection and how to keep your data secure**
- **Ownership of data, copyright and plagiarism**
- **Defamation, harassment and other unacceptable behaviour**
- **Privileged or confidential information**
- **Bringing the University into disrepute**
- **Take Down procedure**
- **Service reliability**
- **Longevity/retention of data**
- **Passwords and using & maintaining ant-virus software**
- **Other sources of guidance and advice, including relevant University policies**

Generally, if your personal internet presence does not make any reference to Edinburgh Napier University, its staff, students or other members of the University community then the content is of no concern to the University. If you do wish to refer to the University, any member of its community or any person with whom you come into contact in the course of your professional studies you must be aware that:

- any information posted must comply with the University's policies on Data Protection and Information Security.
- if you infringe intellectual property rights or post something that is defamatory, you will be personally legally responsible and in doing so you may also breach a University policy or procedure, which will result in disciplinary action being taken against you
- if you are on a course which may lead to a professional registration, the relevant professional body may publish contrary or additional guidance which you must also consult and if you are found to have breached any of the University's Regulations this may have fitness to practise implications for you

Further information is contained in your programme handbook.

KEY POINTS

Data Protection and security of data

- You must not include personal data e.g. contact details or pictures of other students or any other member of the University community without their prior permission. You should respect the privacy and feelings of others.
- The laws which apply to traditional media, such as libel and defamation, apply equally online and you should be aware of this when posting any material, including private correspondence which subsequently enters the public domain (i.e. an MSN chat log which is later published on a blog). Equally, you should be aware that 'locked' profiles (such as on Facebook) are private, but any material you publish to another profile will be classed as public domain if that profile is not locked.
- You are personally responsible for any material identifiable as by your authorship, including by name and also material posted anonymously or under a pseudonym (or username) which can be traced back to an IP address for which you are, or were, responsible.
- Don't post anything that you wouldn't want the public to see about you or which may make you vulnerable - this includes photos or personal details like your address, which may lead to you being inappropriately targeted. The more information you make available the easier it is for unscrupulous people to take advantage of you.
- The internet is a permanent archival system. Be aware that potential employers may search sites to check on job applicants.
- Look at what the service provider's privacy policy is about disclosing your data and decide whether you are content with this. Some sites may share information such as email addresses or user preferences with other companies, which could lead to an increase in spam.
- Most sites will store 'cookies' on your system. Whilst most of these are harmless, some may be malicious. It is advisable to clear your Cookie Cache regularly. Some cookies store a high level of personal information and it is advisable to clear your cookie cache prior to logging out of public access computers.
- Take advantage of a site's privacy settings - some sites may allow anyone to see your profile. Be cautious when deciding which applications to enable and check your settings to see what information the applications will be able to access. **E.g. there has been much publicity recently about Facebook's privacy policy and you should be aware of what this means for you.**
- Locate the policy for handling referrals to make sure that you don't unintentionally sign your friends up for spam - some sites will continue to send email messages to anyone you refer until they join.
- Check whether your data can be retrieved from the system in a form that would allow it to be transferred and used elsewhere or whether you are locked in to the service
- Check the service provider's arrangements for protecting your data from accidental or deliberate access, amendment or deletion AND for backing up your data. Consider what guarantees they offer and whether they are adequate for your needs.
- Check whether you can control what people can do with, and to, your information at a sufficiently detailed level

Ownership of data, copyright and plagiarism

- When you contribute to a site in the course of your studies you must consider the copyright of your contribution. This may include not only extracts or quotes from published reference materials but also images and video/audio clips.
- If you don't have written permission to use material then you mustn't use it. If you have permission you must be sure to correctly attribute the original creator.

- Don't use images from blogs, online newspapers or sites such as Google Images unless the terms and conditions of the site hosting the resource explicitly permit its reuse.
- Although you may own all of the content and information you post on Facebook and can control how you share your content through your privacy and application settings, you should consult Facebook's Statement of Rights and Responsibilities: <http://www.facebook.com/terms.php> for comprehensive information about e.g. the site's use of certain types of content.
- You should also be aware that you need to seek consent from other subscribers before you use any of the information they have posted.
- See also YouTube's terms of service: <http://www.youtube.com/t/terms>
- Be aware that plagiarism may be detected from participating in or viewing online collaborations or academic discourse in the online environment. Information on how the University will use the text matching service Turnitin[®]UK and the essay marking tool GradeMark[®] UK is available on the *Be Wise, Don't Plagiarise* site at: <http://www.napier.ac.uk/ed/plagiarism>

Defamation, harassment and other unacceptable behaviour

You must not use a site to:

- abuse or make defamatory statements about University staff, students or other members of the University community
- express, present or permit violent, indecent, disorderly, aggressive, threatening or offensive behaviour or language towards a member of the University community
- electronically distribute or publish a poster, notice, sign or publication of material of any nature which is threatening, abusive, insulting, obscene or offensive, or may constitute harassment, makes others fear violence or is illegal
- Advertise, for sale or otherwise, items which are prohibited by law or which, by redistribution, would breach copyright or other legal protections
- Advertise the sale of goods or services from within any University property, including student accommodation

Be aware that material which you may not consider to be "offensive" may well be regarded differently by those receiving, witnessing or being subjected to it. You should not use an online forum to criticise, embarrass or humiliate another student, member of staff, group or department. The University has procedures in place for you to raise legitimate complaints, more information about which is available at:

https://studentportal.napier.ac.uk/studentaffairs/studentwellbeing/appeals_complaints_conduct/complaints/Pages/default.aspx

Privileged or confidential information

You must not deliberately disclose privileged or confidential information about the University (including details of internal University discussions) its staff, students or other members of the University community. If you do disciplinary action will be taken against you.

Bringing the University into disrepute

- You must avoid bringing the University into disrepute in any way, as this may constitute a breach of the Student Disciplinary Regulations. If you have a complaint about your course or are dissatisfied about some other aspect of your student experience you should refer to the Student Complaints Procedure and raise your complaint with the appropriate University personnel

- Please remember that you do not have the right to brand external web pages using the University's identity or logo or otherwise to appear to represent the institution in any way when you are not authorised to do so.
- If someone from the media or press contacts you about posts on your site which may have implications for the University, you should take advice from Corporate Communications before you respond

Take down procedure

You should be aware that you may be required to take down or delete information that you have posted to a web 2.0 service for a variety of reasons (e.g. defamation, or where there has been a breach of copyright or the Data Protection Act) and that you may be subject to disciplinary action under the Student Disciplinary Regulations.

Service reliability

If you are responsible for setting up or choosing your own external service the onus is on you to check the following:

- Will the external service be available as required e.g. if it's based overseas or has scheduled or unscheduled downtime during term time?
- Will you be relying on a service whose conditions and terms of use may change sporadically or which may even cease trading, change ownership or become fee paying?
- What will happen if updates don't take place, features suddenly disappear or site support becomes unavailable?

Please note that the University's C & IT Services do not provide support on externally hosted sites

Longevity/retention of data

- Check what the service provider's policy is regarding "idle" data and whether you can be assured that it will not be deemed abandoned and thus deleted
- Investigate what will happen to your data when you decide to delete it. Remember that once you post information online you can't retract it and that saved or cached versions may still exist on other people's machines
- Consider what arrangements the service provider offers for long term retention of data with changes in technological, software and data standard changes

Passwords and using & maintaining anti-virus software

- Protect your account with strong passwords that cannot easily be guessed; a compromised password means someone else may be able to access your account and pretend to be you.
- Anti-virus software recognises most known viruses and protects your computer against them, so you may be able to detect and remove the virus before it can do any damage
- Keep virus definitions up to date.

FURTHER INFORMATION AND REFERENCES

UNIVERSITY POLICIES, GUIDELINES AND REGULATIONS:

Data Protection Code of Practice:

<http://staff.napier.ac.uk/services/CorporateAffairs/governance/DataProtection/CodeofPractice/Pages/default.aspx>

Information Security Policy:

<http://staff.napier.ac.uk/services/cit/infosecurity/Pages/InformationSecurityPolicy.aspx>

Intellectual Property policy:

www.napier.ac.uk/aboutus/foi/publicationscheme/Documents/Forms/DispForm.aspx?ID=12

Referencing, Plagiarism and Copyright Guidance:

<http://www2.napier.ac.uk/inform/main.html>

Harassment and Bullying Policy:

<http://staff.napier.ac.uk/services/hr/hrdocuments/Pages/Documents.aspx>

Netiquette guidelines:

<http://www2.napier.ac.uk/webct/students/netiquette.htm>

The Student Disciplinary Regulations and Student Complaints Procedure:

https://studentportal.napier.ac.uk/studentaffairs/studentwellbeing/appeals_complaints_conduct/Pages/document_library.aspx

EXTERNAL SOURCES

Please note that all links provided in this guidance to sites operated by third parties are for your information and convenience only. Edinburgh Napier University has no control over these sites and accepts no liability in respect of their use.

The UK Information Commissioner (ICO) gives guidance on protecting personal information and social networking at: <http://www.ico.gov.uk/youth.aspx> and on protecting your personal information online at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/protecting_your_personal_information_online.pdf

The BBC has also published guidance at:

<http://www.bbc.co.uk/webwise/guides/protecting-personal-info>

Search photo sharing sites such as <http://flickrcc.bluemountains.net/>, which make images available under an alternative licensing scheme known as Creative Commons: <http://creativecommons.org/>. **Please ensure that you read carefully and follow the guidance on use and attribution.**

JISC Digital Media has published for quick reference purposes only a set of FAQs at: <http://www.jiscdigitalmedia.ac.uk/stillimages/advice/frequently-asked-questions-about-copyright/> for publishing images in virtual learning environments or on websites.

Edinburgh Napier University gratefully acknowledges the assistance of JISC Legal and UCLAN in the development of these guidelines.