WEB 2.0 SERVICES AND OTHER EXTERNALLY HOSTED SERVICES

GUIDANCE FOR STAFF IN LEARNING AND TEACHING

Summary

Web 2.0 Services, such as wikis, blogs and social networking sites (e.g. Facebook, Twitter) provide you and your students with valuable educational opportunities to create and share content and work online together. However, you must be aware of the important legal and other implications that arise if you plan to use Web 2.0 services as part of your module activities and communicate these effectively to your students and other users. Links to guidance provided by JISC Legal for professional service users of externally hosted services are given at the end of this guidance.

This guidance will:
- assist you in making the most of Web 2.0 Services and other externally hosted services for learning, teaching and assessment purposes
- make you aware of the relevant legal and compliance issues; and
- help to protect both the reputation of the University and our students in their use of these services.

Please note that staff are encouraged firstly to consider using internally hosted services and should contact the Web Services Team via the IS Service Desk for advice on these.

Introduction

This guidance covers what you need to consider for externally hosted services in respect of data protection, intellectual property rights, legal and accessibility issues and provides a link to illustrative worked examples at:
https://staff.napier.ac.uk/services/vice-principal-academic/academic/TEL/Pages/web2.aspx

Higher Education Academy (HEA) have published guidance on Web 2.0 services here:

Thereafter if you have any major concerns about your proposed use of an externally hosted service, you should raise these with your Head of School or Director of Service.

The Data Protection issues

These are:
- What you need to do if you're proposing to use an external service provider
- How to advise users clearly about the information that will be published and what will be made available on a restricted basis
- How to transfer personal data to third parties outside the EEA
- How to inform contributors to a University hosted external service about the terms and conditions of the use of the site and their rights to opt out of certain activities
- What to do to ensure that you don't use a service that may expose either the University to liability for breach of Data Protection Legislation (GDPR and DPA 2018) or users to unwanted long term personal data disclosure

1. The role of the service provider

If you are considering using an externally hosted service then the University will be legally responsible for any breaches of Data Protection Legislation if:

- The University has negotiated a specific agreement with the service provider
- The service is branded as a University service
- It is not immediately apparent to users of the service that they are providing data to an external service provider rather than to the University
- Students must sign up to the service as a compulsory requirement of a course or programme
- The service provider can only use the data in ways or for purposes specified by the University

You can take steps to avoid the University becoming legally responsible by:

- Making participation in and contribution to the service optional for users – i.e. it is not a compulsory element in the programme and users can choose whether or not to contribute (e.g. to a wiki). You should also consider what could be offered as an alternative. (see also 2. below)
- Clearly identifying that the service is provided by an external service provider, both on the site itself, in any supporting institutional documentation (e.g. programme handbooks) and in the way that the users access the service (e.g. if students enter the site from Moodle, that they are given a message that they are now leaving the institution's service and connecting to an external service provider)
- Providing students and other users with clear guidance on what information is accessible to and used by the University and what information is accessible to and used by the service provider
- Ensuring users of the service sign up to use the service directly with the service provider and not through the University. In this way, each individual can decide on the extent to which they wish to establish their own relationship with the service provider, and can withhold or disclose whatever personal information they wish

If you are proposing to use an external service provider you should ensure that you do the following:

- Consider – in consultation with your Head of School/line manager - whether an agreement needs to be in place with the provider and then take advice where necessary from the Information Governance Manager
- Where users are to register individually, check that the terms of the service which users will be signing up to are appropriate for the UK legal environment. This is particularly important where you are considering making use of the service compulsory for a course. See also sections 2-5 and Legal Issues below.
- If the terms of use are not clear contact the service provider and seek clarification
- Users must not be required to sign up for a Web 2.0 service that may breach UK data protection legislation and you should check whether users will be required to waive legal protections guaranteed by UK law. Sections 2 to 5 below give further specific guidance on this.
- Provide clear guidance either by a short briefing to students or in the relevant programme handbook and/or programme Moodle site about the data protection implications of their registration. You should include in this advice on the effective use of privacy enhancing elements of the service and how to unsubscribe and remove personal data from the service

## 2.	Publication of personal information

Use of some Web 2.0 services may involve requiring users to publish their personal data on the Internet. You must be aware that compulsory use of such services by the University, or use of such services in circumstances which place users who do not wish to make such disclosures at a significant disadvantage, may breach Data Protection Legislation. You can avoid this by using services which let users conceal their identity, e.g. by allowing the use of aliases. However, it is recommended that because of potential problems in assessing students you should set up in advance and retain for future reference the list of aliases. In addition, withholding of names does not equate to anonymising data, and you should be aware therefore of the risk that in requiring the disclosure of so much information a user can be identified even in the absence of their name. You must clearly advise users about what information will be published and what will be available on a more restricted basis.

## 3.	Transferring personal information outside the EEA

Many Web 2.0 service providers are based outside the European Economic Area (EEA), e.g. in the United States. While it is acceptable for individuals in the EEA to choose to supply their personal data to non-EEA service providers, Data Protection Legislation prohibits the transfer of personal data by the University to third parties outside the EEA, unless certain conditions are met.

Where you propose to use a Web 2.0 service provider, you must ensure that users will know where information that is supplied to the service provider will be processed, so that appropriate measures can be taken. Methods of dealing with personal data transfers outside the EEA in circumstances where a web service is to be used are:

- Where users have a choice whether or not to sign up, you should ensure that users are adequately informed about the data protection consequences of doing so
- Where the user registers directly with the service, s/he is aware of the overseas transfer, and has control over what information is provided to the service provider; you must ensure that users are adequately informed about the data protection consequences of doing so

4. Information provision where the University collects personal data

In order to comply with the relevant legislation, where you use an external Web 2.0 service provider to collect information about or contributions from people on its behalf, you must provide clear information, preferably in the programme handbook about:

- How the University or other parties will use the information
- Who will have access to or will retain copies of the information
- What information will be generally accessible over the Internet
- Any cookies that may be downloaded to the user's computer
- Any monitoring of an individual's usage and activity in the service
- The country that hosts the service if this is outside the UK

In addition you should ensure that:

- Users must be able to opt out of the use of cookies and monitoring.
- If an externally-provided service is designed to appear to be part of the University (e.g. a template has been used to apply the University's branding to a blog) people who register at that site (e.g. in order to post comments to the blog) understand that they are not just entering into a relationship with the University but also with the service provider.
- You give users clear information about what information is available to, and used by, which party.
- You avoid using services where it is not possible to opt out of advertising and marketing emails. To minimise the risks of breaching the relevant legislation, you should give users clear instructions on how they can opt out of advertising and marketing activities if they wish to do so.

5. Information retention

Personal data placed on Web 2.0 services based in non-EEA countries may, in some circumstances, be legally held indefinitely and the service providers may have no legal obligation to remove it. Data Protection Legislation requires that information about individuals should be kept no longer than necessary. You should therefore:

- Consider whether the Web 2.0 services you want to use will expose the University to liability for breach of Data Protection Legislation or expose users to unwanted long-term personal data disclosure
- Ensure that the Web 2.0 services you wish to use have adequate data privacy guarantees concerning the appropriate removal and disposal of users' personal data after the purpose for which it was collected and processed has ended
- Note the University's recommended retention periods for student coursework: https://staff.napier.ac.uk/services/governance-compliance/governance/records/Pages/RecordsRetentionSchedules.aspx

Legal Issues

1. Take Down policy

Before signing up to a service, you should consider whether you have sufficient control over content, and the terms of use and facilities of the external service will permit you, to

take down or delete any illegal or inappropriate postings, particularly where there is a link in any way to the University. This could apply e.g. where there has been a breach of Data Protection Legislation, an infringement of copyright or where a defamatory statement has been made.

2. Copyright and other intellectual property issues

These are:

- **What you need to consider before you put copyright material online**
- **What permissions you and your students must obtain**
- **What you need to be aware of with potentially patentable inventions**
- **Who will own the copyright of any material that is created**

Copyright

- You must consider whether you have the necessary permissions to put copyright material online. You may be personally liable for copyright infringement and the University may be liable for your acts as an employee.
- You must not permit students to put copyright material online without permission or statutory exception. At the very least this will be bad practice and at worst it could lead to the University being liable where students are acting under the direction or instruction of the University.
- You must also consider whether you are permitted to copy designs, a database or other intellectual property protected resources. Designs may be subject to intellectual property rights, as might databases.
- Remember that there may be a number of intellectual property rights to consider e.g. a CD involves copyright in the disc's cover, copyright in the musical composition and the lyrics, performance rights and rights in the recording. These all need to be cleared where relevant and may not be held by one person or body.

Patents

Inadvertent disclosures on a discussion list e.g. about a potentially patentable invention could lead to details being made known to the public. As a patent will not be granted if details are made public prior to the patent application, this could have serious financial consequences and prevent either the University or a partner body from obtaining a valuable patent.

Intellectual property rights

- Particularly in the case of collaboration, or the creation of resources for re-use or with a potential commercial value, you must make it clear who is to own intellectual property in the output created using Web 2.0 technologies. You will need to take particular care where you require students to assign their intellectual property rights to the University as this may be invalid in law. (See section 2.4.2 of the University's Intellectual Property policy)
- In accordance with the University's Intellectual Property policy, copyright in materials created by you in the course of your employment will belong to the University unless there is an agreement otherwise.

3. Liability issues

These are:

- **Consider what will happen if the service is withdrawn during a programme**
- **Be aware of the types of potential misuse by users**

- In selecting an externally-hosted technology you must consider the implications should the service be withdrawn during term time. Students may have an action against the University if their learning is disrupted through the negligence of the University, its employees or agents or in breach of a contract. You may need to make a judgment as to the durability of each particular technology.
- You should ensure that you set out limits as to what behaviour is acceptable, consider moderation of content and what steps would be reasonable to prevent misuse by the posting, storage or dissemination of inappropriate and possibly illegal content.
- You must be aware that an external service could also be used as a tool for bullying, harassment or defamation. The University could be legally liable where it is negligent in allowing Web 2.0 facilities to be used inappropriately.
- On becoming aware of any potential liability attaching to the University, you should inform your Head of School or Director of Service immediately of the circumstances

If after you have read through this guidance and taken appropriate advice, you decide to make use of a selected service compulsory, you should be aware that you will be personally responsible for the consequences of any legal or compliance breaches which may arise.

4. Reputational Damage

You must ensure that there is appropriate consultation with your Head of School/line manager before you sign up to technology where there may be sensitive issues which could damage the reputation of the University or any partner organisation. Breach of the terms and conditions of the site will mean some level of legal liability, will introduce uncertainty as to whether the use of the tool or site could be withdrawn with disruption to the students' learning and may prevent dissemination of what would otherwise be a good example of teaching and learning innovation.

5. Accessibility

You must not place students with disabilities at a disadvantage in the selection and use of any Web 2.0 or other externally hosted service. You must consider in advance therefore whether any technologies chosen can be adapted to meet the needs of all users with disabilities in order to meet our obligations under disability discrimination legislation and ensure accessible learning for all. For more information on accessibility contact the Wellbeing and Inclusion team:
https://staff.napier.ac.uk/services/Student-Wellbeing-Inclusion/Pages/StudentWellbeing.aspx

This guidance has been adapted and developed from material published by JISC Legal Governance and Management Services/September 2018

6

FURTHER INFORMATION AND OTHER UNIVERSITY RESOURCES

The University's Data Protection Code of Practice:
https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/CodeofPractice/Pages/default.aspx

Guidance for Students on the Internet, Web 2.0 and other externally hosted services:
https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/InternetServices.aspx

The University's Intellectual Property policy and guidance on copyright:
https://staff.napier.ac.uk/services/research-innovation-office/policies/Documents/Intellectual%20Property%20Policy.pdf

Copyright Information:
https://staff.napier.ac.uk/services/library/teaching/Pages/copyright.aspx

The University's Information Security Policy:
http://staff.napier.ac.uk/services/cit/infosecurity/Pages/InformationSecurityPolicy.aspx

Information on internally-hosted services:
Contact the Web Services Team via the IS Service Desk
Information for staff on internally-hosted services can be found at:
https://blogs.napier.ac.uk/learningtechnologyhub/

For further advice contact Governance Services:
☎**:** 0131 455 6257; 🖱**:** dataprotection@napier.ac.uk

EXTERNAL RESOURCES

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 University of Edinburgh's guidance is regarded as an exemplar for the HEI sector:
https://www.wiki.ed.ac.uk/display/Web2wiki/Web+2.0+Guidelines

JISC Legal: www.jisclegal.ac.uk

JISC Technology and Tools for Online Learning:
https://www.jisc.ac.uk/full-guide/technology-and-tools-for-online-learning

Intellectual Property Rights guidance at: https://www.jisc.ac.uk/guides/intellectual-property-rights-in-a-digital-world