University of Edinburgh
Information Services
Guidelines for Using External Web 2.0 Services

Reuse or distribution: This document is subject to the Creative Commons Attribution 3.0 Unported Licence (http://creativecommons.org/licenses/by/3.0/). The "Original Author" of the document is The University of Edinburgh, and section 4(b) of the License requires you to acknowledge the University in any "adaptation" you create.

Please note the disclaimers in clauses 5 and 6 of the License, and non-UK institutions should particularly note that their legal constraints will be different.

<table>
<thead>
<tr>
<th>Date of release</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 August 2008</td>
<td>Addition of front page and license statement.</td>
</tr>
<tr>
<td>23 August 2007</td>
<td>First publicly-accessible version.</td>
</tr>
</tbody>
</table>

Feedback on this document should go to C.J.Adie@ed.ac.uk.
1 Introduction

Traditionally, the World Wide Web has been a one-way, publisher to reader, medium. The distinguishing feature of Web 2.0 is that it is a bidirectional medium, where content (text, image, audio or video) is contributed by people who interact with the website as well as people and organizations who manage the site – in other words, it is the “read/write web”.

There are many companies on the Internet offering attractive and useful applications services based on the Web 2.0 paradigm, including blogs, wikis, office systems, social bookmarking etc – and of course there are virtual worlds such as Second Life which transcend the definition of “Web 2.0”. These are increasingly being adopted by computer users within the University, for administrative, teaching, learning and research purposes.

This document offers guidance to staff within the University on some of the issues which need to be considered before using such services for University purposes. The document is intended to be helpful for all staff, including researchers, teaching staff and support staff. Note, however, that it focuses on issues specific to using external Web 2.0 services – issues which are common to Web 2.0 services regardless of whether they are internally or externally hosted are not specifically addressed.

The University’s use of Web 2.0 services\(^1\) is developing quickly, and the services themselves are changing and expanding even more rapidly. It is inevitable that the information herein will be far from a complete or comprehensive guide to the issues. You should therefore seek other relevant advice and use your own common sense as well as relying on this document.

After outlining some of the potential advantages of and concerns about using external Web 2.0 services, specific issues relating to the suitability of the service for your requirements are described. Detailed implications of current legislation and University regulations are discussed. The main concepts of Risk Analysis are presented, and a template Risk Assessment is presented for you to fill in.

We believe that this University is leading the way in developing guidelines for using external Web 2.0 services. We will inevitably make mistakes, and it is important that you provide feedback if you find that the guidelines are inadequate, or if you have had experiences about which others should be warned.

It need hardly be said that this document comes with no guarantees, and certainly does not constitute “legal advice”!

\(^1\) For the purposes of this document, the term “Web 2.0 services” is meant to include systems such as Second Life.
2 Pros and Cons

What makes the use of external services attractive? Reasons include:

✓ “It’s easy to make use of the latest technology. Information Services can’t possibly provide every kind of Web 2.0 service I’d like to use.”

✓ The social aspect of many services is predicated on very widespread usage – there is no point in the University trying to replicate del.icio.us or Facebook for example.

✓ It’s extremely quick to get an account and check out a service. Often it’s free for basic functionality, and cheap for more advanced functionality.

✓ “I can easily get my students/colleagues/research partners to sign up for the same service so we can collaborate.”

✓ “Internally-provided services don’t fit my needs as closely as a selected external service.”

✓ “My research partners are using an external service and in order to collaborate I need to use it too.”

✓ Using an external service may make it easier for students to retain access to the work they’ve produced when they leave the University.

There may be perfectly valid reasons for using external services; however it is important that, when making the decision to use such services, you recognise the downsides too.

✗ The service provider company may change the nature of its service or may even cease trading.

✗ Your information could be at greater risk of unauthorised use or loss than if you hold it within the University.

✗ If the service is hosted in a different time zone, support may not be available when you need it, and scheduled maintenance may make the service unavailable at an inconvenient time of day.

✗ As just one among many tens of thousands of customers, you have much less influence on the development of the service.

✗ It may be difficult to show that you are complying with relevant UK legislation and University regulations.

These issues are considered in greater detail below.
3 Service-Related Issues

Some of the concerns about using external Web 2.0 services will relate to the specific activity you are planning, and the specific service you are planning to use. The appropriate response to these concerns will differ from case to case.

3.1 Security of Service Provider

Will the company still be around in six months (or even one month)? Many Web 2.0 companies are comparatively small, and regularly come and go – see the TechCrunch Deadpool² for some of those that have gone. Even if a company does not cease trading, changes in ownership may seriously affect the business. What would happen if your Web 2.0 service provider gets bought by a competitor or a much larger company?

3.2 Confidentiality

What is the service provider’s policy about disclosing your data, and do the policy and any associated guarantees satisfy your needs? There are legislative requirements, which are covered later in this document, but your project may have specific additional requirements for confidentiality – for instance, if valuable intellectual property is being developed as part of a research project. Similar issues apply if you wish to upload licensed content to the web service: it’s vitally important to check the terms of the license.

Note that exposure of confidential information is not a theoretical risk – e.g. a recent high-profile disclosure of search data by a major web search engine provider allowed the (sometimes embarrassing) searches performed by specific identifiable individuals to be determined.

Search engines can and probably will find out, index and perhaps cache all the openly-accessible information you upload. You may have less control over what is indexed and cached than you would have if the service was hosted locally.

3.3 Ownership of data

You need to consider questions of ownership of information which is entrusted to the service provider.

In order to use some Web 2.0 services (e.g. some discussion boards) you have to agree that your contributions will be subject to the Gnu General Public License (GPL)³ or to a Creative Commons⁴ license. In other cases, users may be required to

² http://www.techcrunch.com/tag/deadpool/
³ http://www.gnu.org/copyleft/gpl.html
⁴ http://creativecommons.org/

© 2007, 2008 The University of Edinburgh
waive certain of their moral rights – for instance the moral right to be identified as the author of their work.

In some cases, the terms of service may require you to grant very extensive rights to the service provider – for instance, in order to use one commonly-used service you must agree to:

“ ...[grant] ... the royalty-free, perpetual, irrevocable, non-exclusive and fully sublicensable right and license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform and display such Content (in whole or part) worldwide and/or to incorporate it in other works in any form, media, or technology now known or later developed...”

If you are planning to use the service for research information, or even for teaching material, this may be an unacceptable condition. Intellectual property rights in created information will often belong to the University, and may well be valuable property which must not simply be given away.

3.4 Security of data

What are the service provider’s arrangements for protecting your data from unauthorised accidental or deliberate access, amendment or deletion and for securely backing up your data? What guarantees do the company offer, and are they adequate for your needs?

Is the level of access control adequate – in other words, can you control what people can do with and to the information at a sufficiently detailed level?

3.5 Performance

If there are performance problems, how ready is the service provider to address them? Are there any performance issues associated with the remoteness of the server (e.g. network bandwidth/congestion issues), which lie beyond the ability of the service provider to address?

3.6 Reliability

Is the service available as required, or does it have scheduled or unscheduled downtime? What would the impact be if this occurred in the middle of semester or the middle of a class practical? For instance, if a US-based service is performing maintenance operations at 0300 PST, that may affect system availability at 1100 UK time.

Note that the risk of the service being unavailable increases the further away it is – compared to a local service, much more network infrastructure needs to be working if the service is located in California.

http://sourceforge.net/docman/display_doc.php?docid=6048&group_id=1
3.7 Support

Service provider support may be from an inconveniently-different time zone. Is overnight turnaround on support calls acceptable? How much local (UoE) knowledge and support is available?

3.8 Single sign-on

It is not possible to extend the University’s EASE single-sign-on mechanism to external services (at least, not without negotiating a special contractual arrangement with the service provider, even if it were technically possible). This means that you, and anyone else who is involved with using the service as part of your project, may need to create a new identity on the service provider’s site, and remember another password.

It cannot be emphasised enough that passwords you use for external websites MUST be different from your EASE password.

3.9 Lock-in

Can your data be retrieved from the system in a form which would allow it to be transferred and used elsewhere, or are you "locked in" to the service? With the wide variety of differing services on offer, it is probably the case that suitable standard formats will not always exist. Furthermore, support for exporting your data to allow it to be moved to a competitor’s service will be low on the priority list for many Web 2.0 companies. How important is avoiding lock-in in your case?

3.10 Longevity

In some cases, the longevity of the information on the service may be important – what is the service provider’s policy regarding “idle” data, and can you be sure it won’t be deemed to be abandoned and therefore deleted?

If you need to keep the information for many years (e.g. because of research funding council policy on data retention), does the external service provider have arrangements in place to ensure the long-term survival of the data despite risks such as technological obsolescence and software and data standard changes? Would it be better for you to make arrangements to preserve the data yourself?

3.11 Functional stability

You should approach choosing a web service provider with the same care that you would in choosing any commercial software package or service. You need to assure yourself that the functionality, usability, accessibility etc on offer will satisfy your needs.

However, there is a significant difference between a web-based service and a commercial software package. The service provider can choose to alter the functionality of the service, or indeed its terms of use, privacy policy, charging policy, prices etc. Unlike a desktop software package, you don’t have the option of remaining with a previous version of the software if you don’t like the new version.
If a service provider notifies you (e.g. in an email newsletter) that its terms of service have changed, you MUST check whether the change affects your risk assessment of any of the issues mentioned in these guidelines.
4 Legislative and Regulatory Issues

4.1 Data Protection and Freedom of Information

The Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002 apply to information held by the University or held by an organisation providing services on behalf of the University. The legislation gives valuable protection to the rights and freedoms of individuals, including students and researchers. Failure to comply with it can result in the University being sued, or in damage to its reputation. In almost all cases, it is quicker and simpler to avoid difficulties by addressing compliance issues when setting up a service, rather than waiting to deal with potential non-compliance issues when they arise.

The Data Protection Act applies to information about individuals (“personal data”). When using externally-provided Web 2.0 services, it is almost always necessary to use personal data – for instance, the user’s email address, name, perhaps their address, personal interests etc – so in most cases the Data Protection Act requirements will apply.

The service-related issues identified in section 3 also have legal compliance implications. This section will focus on the main requirements of information legislation as it applies to the use of externally-provided Web 2.0 services. Further advice is available from the University’s Records Management Section (recordsmanagement@ed.ac.uk).

If you enter into an arrangement with an external service provider for the provision of Web 2.0 services, the following are the principal information legislation risks:

4.1.1 Service Provider as a Data Processor

Are the terms of the arrangement such that the University becomes legally responsible for any breaches of the Data Protection Act committed by the service provider? This will occur if the service provider is explicitly contracted to provide particular services for the University in such a way that (in data protection terms) they become a data processor acting on behalf of the University. Indicators that this may be the case include:

- You have negotiated a specific agreement with the service provider.
- The service is branded as a University of Edinburgh 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.
- Sign up to the service is a compulsory requirement of the course or programme.
- The service provider can only use the data in ways or for purposes specified by the University.
In such cases you must ensure that there is a contract between the service provider and the University covering the relevant legal obligations. The Records Management Section website\(^6\) includes sets of model contract clauses that you can use in such a case. The page includes a flow chart that will help you to decide which clauses are most appropriate in your circumstances.

If possible, avoid becoming legally responsible for the service provider’s compliance with the Data Protection Act by ensuring that it is clear that the service provider is a separate legal entity over which the University has no control. Indicators that this may be the case include:

- It is clear that the service is provided by an external service provider, both on the site itself, in any supporting University documentation (e.g. course handbooks) and in the way that the user access the service (e.g. if students enter the site from WebCT, that they are given a message that they are now leaving the University of Edinburgh and connecting to an external service provider).

- Users of the service, such as students, are clearly told what information is accessible to and used by the University, and what information is accessible to and used by the service provider.

- 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.

- Participation in and contribution to the service is optional to users – e.g. users can choose whether or not to contribute to a research wiki.

- The University has no control over the uses to which the service provider puts the data.

If you plan to ask users to register individually, you should check beforehand that the terms of service which people will be signing up to are likely to be acceptable to them. This is particularly important where use of the service is compulsory for a course. It is recommended that, when you invite people to register at a website, you warn them about the risks of disclosing personal information to external services. These include the risk of exposure to unsolicited marketing and spam, the impact on intellectual property rights, the potential for the exposure of personal information to a world-wide audience and differences in attitudes to privacy and the use of data in different national regimes. For a group of students, you may wish to give them a short briefing on the risks at the start of the course or to provide some information in

\(^6\) http://www.recordsmanagement.ed.ac.uk/InfoStaff/DPstaff/TransferringInformation/DataTransfers.htm
the course handbook. Alternatively, it may be appropriate to include this sort of information in a privacy policy.

4.1.2 Publishing Personal Information

The second risk is that the arrangements for using the service are such that users are obliged to publish their personal data on the Internet. In rare situations this could give rise to personal security issues. It could also involve a breach of the Data Protection Act. You can avoid this by using services which let users conceal their identity, e.g. by allowing the use of aliases. Be careful that you do not require users to disclose so much information about them that they are identifiable even if they withhold their name. For example, if you know a person’s gender, age, postcode, occupation and ethnicity then they may still be identifiable even if their name is not disclosed. Use media such as privacy policies or course handbooks to make sure that users are aware what information will be published and what information will be available on a more restricted basis.

4.1.3 Transferring Personal Information Outside the EEA

Do the arrangements for using the service involve the transfer of personal data outside the European Economic Area? For example, the service provider or its parent company might be based in the United States. You can check this by reading any information the service provider makes available about their organisation, or by looking for clues such as the legislative regime specified in the service agreement. If the agreement specifies US legislation, then it is quite likely that the service provider is based there. The Data Protection Act prohibits the transfer of personal data outside the European Economic Area unless certain conditions are met. You can avoid this difficulty in a number of ways:

- by using a standard web service which users sign up to at their own choice.
- by arranging the use of the service so that the user registers directly with the service, is aware of the overseas transfer, and has control over what information is provided to the service provider.
- by negotiating a customised agreement with the service provider\(^7\), making use of the model contract clauses available at the Records Management Section Website.

Do not supply personal information about other people (students, colleagues, anyone at all) to external websites unless you have the consent of the people concerned, as in some circumstances this may be a transfer of personal data outside the European Economic Area. (For instance, using yousendit\(^8\) to send a large database file containing people’s names and addresses to a colleague may fall foul of the Act.) If

---

\(^7\) This may not be a practical option for low-value services where the supplier is making little profit from your use of the service.

\(^8\) http://www.yousendit.com/
you definitely need to do this, you should contact the Records Management Section (recordsmanagement@ed.ac.uk) for advice on how to transfer the information legally.

4.1.4 Need for Clarity

A further risk is that users are unclear as to what information they are providing to whom. Under the Data Protection Act and related legislation, if you use an external service provider to collect information about or contributions from people on your behalf, you must provide clear information as to how you or other parties will use the information, any “rules” governing the contributions, 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 and (if the service is hosted outside the UK) the country that hosts the service. Depending on the nature of the use you are making of the service, appropriate mechanisms for doing this include privacy statements or course handbooks. A best practice example of a privacy statement can be seen at the Personality Rights Database. Users must be able to opt out of the use of cookies and monitoring.

If you have arranged for the externally-provided service to appear to be part of the University (for example, if you have used a template to apply University branding to a Blogger blog) then you need to be particularly careful to ensure that people who register at that site (e.g. in order to post comments to your blog) understand that they are not just entering into a relationship with the University, but also with the service provider. You must give them clear information as to what information is available to and used by which party. See below for further information about University branding.

4.1.5 Information Retention Policy

Will personal information be kept for longer than is necessary by the University or by a data processor acting on the University’s behalf? The Data Protection Act requires that the University or organisations acting on its behalf keep information about people for no longer than necessary. Guidance on the necessary retention periods for common types of University records is available at the Records Management Section website. You should, therefore, consider if it is possible to delete or take down information once your need for it has ended.

4.1.6 Notification and Takedown Policy

You might need to take down or delete information that has been posted to a Web 2.0 service for a range of legal reasons, including defamation, breach of copyright, or breach of the Data Protection Act through the processing of information likely to


10 [http://www.blogger.com/](http://www.blogger.com/)

11 [http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/RMguidance.htm#RetentionSchedules](http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/RMguidance.htm#RetentionSchedules)
cause someone substantial damage or distress. Before signing up to a service, consider whether the terms of use and facilities of the external service will enable you to do this quickly, if necessary.

4.1.7 Unsolicited Messages

The service provider may make use of user’s details for advertising and marketing purposes. This can be annoying for users and, in cases where use of the service is compulsory or where the service provider is a data processor acting on behalf of the University, might lead to difficulties under the Privacy and Electronic Communications (EC Directive) Regulations 2002. To minimise these risks, ensure that you give users clear instructions on how they can opt out of advertising and marketing activities if they wish to do so. Avoid using services where it is not possible to opt out of advertising and marketing emails.

4.2 Accessibility Legislation

The Disability Discrimination Act 1995\textsuperscript{12} and subsequent amendments places significant responsibilities on the University, and it is important to ensure that by using an external service, you are not placing the University in breach of its responsibilities.

The level of accessibility of external websites will vary. Regulations and expectations in the country where the website is hosted may be different from the UK, so be aware that service provider claims of “accessibility” may not necessarily be adequate. You may wish to seek advice from the Disability Office.

4.3 Other University Regulations

4.3.1 Assessment

Some material stored on or in external services could be the basis for assessing students – for instance an external blog, or a building or artefact in Second Life. The University regulations on assessment\textsuperscript{13} should be read in the light of what you plan to do – in particular, they state: “Assessment processes must ensure the security of their operation in terms of the safe recording, transfer, storage and retrieval of information on student achievement.”

You need to be clear to students about what the University’s responsibilities are, and what the students’ responsibilities are. Some of the considerations you need to bear in mind include:

- How do you ensure that no changes can be made to the material after the submission deadline?

\textsuperscript{12} http://www.disability-office.ed.ac.uk/legislation/dda_general.cfm

\textsuperscript{13} http://www.aaps.ed.ac.uk/regulations/exam.htm
• What level of visibility does the work have to other students, and is this appropriate?

• What would you do if a student alleges that they submitted work but “it’s not there now”?

• What is the impact if the external site is unavailable for some reason?

• How long will you need to keep the assessed material? (The University’s Assessment Regulations state, “Material which contributes significantly to the overall assessment of the course, including degree examination scripts, should be retained in the School for four months after the Board of Examiners meeting. This may be the resit Board of Examiners”\textsuperscript{14} Will the external website still be around by then?

4.3.2 Branding

In some cases you may wish to use branding in externally-hosted sites. For instance, the University has a branded presence in MySpace.

Permission to use University branding on an external site must be sought from the University’s Communications & Marketing department.

Particular care is needed if University branding is used, because of the risks it poses to the University’s reputation. You should ensure that users explicitly agree not to create content that might cause offence or bring the University into disrepute (Information Services is considering producing a “click-through agreement” for internally-hosted Web 2.0 services, the wording of which might be relevant for this purpose). You also need to ensure that there is a clearly-signposted route for reporting unacceptable content to you, and that if such content is created you can remove it promptly without the involvement of the service provider.

4.3.3 Computing Regulations

Note that the University Computing Regulations\textsuperscript{15} cover the use of external services, but only if accessed through the University network or from University equipment. You should therefore not rely only on the Computing Regulations (in their current 2004 revision) to regulate the use of external facilities by staff or students, since they may use them from home (\textit{i.e.} not using the University’s network or equipment).

There is a risk that information placed on an external service might cause offence or bring the University into disrepute. An appropriate degree of prohibition and


\textsuperscript{15} http://www.ucs.ed.ac.uk/EUCS/regs.html
deterrence is provided by the Student Discipline regulations (regulations III.3 and III.12 are likely to be relevant). For staff, the risk is less and is covered to an appropriate extent by existing regulations or policies. As mentioned above, a “notification and takedown” capability and process is required, to facilitate prompt removal of offending material.
5 Checking the Terms

You should ALWAYS read the terms and conditions for any service you register with. If you are requesting, or requiring, others to register themselves, you should exercise particular care in doing so, and in advising other people about them.

5.1 General checks

Here is a checklist of some of the main things to look out for when reading the terms and conditions.

☐ What sort of intellectual property rights do the terms grant to the service provider?

☐ Who will have access to what information? Is this appropriate?

☐ What measures will the service provider take to keep information confidential? Are these sufficient for your needs?

☐ Is it possible to take down and delete information easily, quickly and permanently from the site?

☐ What are the service provider’s arrangements for protecting your data from unauthorised accidental or deliberate access, amendment or deletion and for securely backing up your data? What guarantees do the company offer, and are they adequate for your needs?

☐ Is the level of access control adequate – in other words, can you control what people can do with and to the information at a sufficiently detailed level?

☐ Does the service provider make any performance guarantees? Are they adequate for your needs?

☐ Can your data be retrieved from the system in a form which would allow it to be transferred and used elsewhere, or are you "locked in" to the service? How important is avoiding lock-in in your case?

☐ What is the service provider’s policy regarding “idle” data, and can you be sure it won’t be deemed to be abandoned and therefore deleted?

☐ If you need to keep the information for many years (e.g. because of research funding council policy on data retention), does the external service provider have arrangements in place to ensure the long-term survival of the data despite risks such as technological obsolescence and software and data standard changes, or is it possible for you to make arrangements to preserve the data yourself?

☐ In which country will the information be held? If it is a country whose respect for the rights and privacy of individuals gives you cause for concern, do not use the service.
What cookies or monitoring of usage does the service provider use? Are they appropriate? Make sure that users are aware of these before they register.

For assessed materials, can you protect them from alteration after the submission date for as long as they are needed?

Does the clause limit the service provider’s liability (and thus the University’s ability to sue the service provider)?

5.2 Requiring others to register

If you are in a position to require others (e.g. students) to register with the service, perhaps as a condition of participating in a course, you must in addition check the following:

Will use of the service expose the users to marketing or advertising material sent to their email address? If so, explain to users how they can opt out of this.

What information will the service provider collect and keep about users? Is it appropriate?

Does the service permit the use of aliases? You should not require people to post information to the Internet if they can be identified from that information.

5.3 Briefing participants

If you are requesting, or requiring, others to participate in the service, you should brief them appropriately at the time you request or require them to do so, using methods such as course handbooks or a privacy policy. Here is a checklist of some of the things you should consider mentioning in your briefing.

Make it clear that the service is provided by an external service provider, giving the provider’s name, contact details and country.

Advise that they read the service provider’s terms and conditions carefully.

Draw attention to any points in the terms and conditions which are particularly significant in the context of your use of the service, including privacy, copyright or IPR terms.

Give clear advice on what information is collected by or accessible to the University, and what information is collected by or accessible to the service provider or to a third party.

Explain what information, if any, will be generally accessible on the Internet.

Describe any “rule” governing contributions to the service.

Give clear instructions on how users can report any material that should be taken down, whether because it is personal information that they do not want in the
public domain, or because it involves defamation, a breach of copyright or other cause for concern.

☐ Advise them on how they can opt out of marketing or advertising material.

☐ Inform users of any cookies or usage monitoring that the service provider uses and how they can opt out of this.
6 Risk Management

A risk can be defined as “a future event (or series of events) with a probability of occurrence and the potential for loss or impact on objectives”. Risk management\(^{16}\) is a systematic process of identifying, analysing and responding to risks. Many of the issues identified in preceding sections represent risks, so risk management is an appropriate framework within which to consider these issues. Indeed, the University has a formal risk management policy\(^{17}\).

6.1 Risk Register

A risk register is a list of risks to the project or activity underway. The risk register will contain a range of information about each risk, the most important being:

- **Description** – This comprises a three-part statement: “There is a risk that X may happen, caused by Y, resulting in Z.”

- **Probability** - What is the likelihood of the event occurring? This might be as simple as “high/medium/low”, where these terms might have specific meaning. The justification for the estimated probability should also be recorded.

- **Impact** - What will the impact on the project or activity (and/or the University in general) be if the event occurs? The justification for the estimated impact should also be recorded.

- **Timescale** - What is the “Risk Window” within which the event may occur, and when do you start to lose options as to how you respond?

- **Response** - What is the plan for dealing with the impact of the event if it does occur? The cost of executing the plan should also be estimated.

- **Mitigation** – What preventative actions can be taken to reduce either the probability of the event occurring or the impact if it does occur? What are the costs of these actions?

- **Residual Risk** – What is the expected level of risk (probability and impact) once all the mitigating actions are complete?

- **Early Warning Signs** - What “trigger” might alert you to the fact that the event is about to occur?

6.2 Using Risk Analysis

How might a risk register be used in practise?

\(^{16}\)http://www.jiscinfonet.ac.uk/InfoKits/risk-management/index.html

\(^{17}\)http://www.aaps.ed.ac.uk/Committees/RiskMgt/Guide/Guide-Contents.htm
One way is simply to use the template provided in the Appendix as an aid to thinking about the risks. If your intended use of an external service is relatively casual (for instance, you want to keep your “to-do” list on an external website), you may simply wish to read through the risk register, thinking about how you might fill it out, but not actually going to the extent of doing so.

On the other hand, if you are planning a high-stakes activity (e.g. depending on an external service as a crucial part of a course) you probably do need to fill it in. For example, suppose you are the Principal Investigator on a research grant, and you would like to manage the research project through the Basecamp\textsuperscript{18} online project management service. Having read through these guidelines, and spoken to your IT support team to check what other options there might be, you decide to complete the Risk Register template (see the appendix).

For each risk, you estimate and record the probability, impact and other factors associated with each risk. You then identify and analyse some further risks specific to this particular research project, and then make a decision (if necessary, in consultation with your Head of School) on whether to go ahead based on your estimation of the benefits of using the service balanced against the risks involved.

During the project, you review the risk register to see whether anything has changed and whether you need to take action to address increasing risks, or reassign resources away from addressing risks of decreasing importance.

At the end of the project, it would be useful if you were to provide feedback on your experience with using the Risk Register, to help Information Services update these guidelines.

Note that if your project is of particular significance to the University, and/or the impact of a risk is severe at University level, you may wish (in consultation with your line management) to consider it in terms of the University’s risk management strategy\textsuperscript{19}.

\footnotesize
\begin{itemize}
\item \textsuperscript{18}http://www.basecamphq.com/
\item \textsuperscript{19}http://www.aaps.ed.ac.uk/Committees/RiskMgt/Remit/MembershipandRemit.htm
\end{itemize}
7 Acknowledgements

These guidelines were formulated by a working party comprising:

Chris Adie, Information Services (convenor)
Paul Anderson, School of Informatics (corresponding member)
Brian Gilmore, Information Services
Susan Graham, University Records Manager
Hamish Macleod, Moray House School of Education
Gill McConnell, Royal (Dick) School of Veterinary Studies
George Ross, School of Informatics
Charlotte Waelde, School of Law

Chris Adie edited the guidelines, and Susan Graham provided considerable material, particularly for the sections on Data Protection and Freedom of Information issues.
**Appendix: Risk Register Template**

The following codes are suggested for Probability (P) and Impact (I). Note that these are expressed in terms which relate to your “project” – a presumed activity of finite duration with specific objectives. You may wish to revise or extend these codes to cope with your particular situation.

<table>
<thead>
<tr>
<th>Probability</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero (Z)</td>
<td>The event cannot occur</td>
</tr>
<tr>
<td>Low (L)</td>
<td>Unlikely to occur (&lt;5%) during the project</td>
</tr>
<tr>
<td>Medium (M)</td>
<td>Significant probability (&gt;5%, &lt;50%) of occurrence during the project</td>
</tr>
<tr>
<td>High (H)</td>
<td>Will probably (&gt;50%) occur during the project</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (0)</td>
<td>No impact (i.e. the risk is not applicable)</td>
</tr>
<tr>
<td>Slight (1)</td>
<td>Minor project objectives will not be fully realised.</td>
</tr>
<tr>
<td>Moderate (2)</td>
<td>Minor project objectives will not be realised, or major objectives will not be fully realised, or there will be some minor loss or damage to the University.</td>
</tr>
<tr>
<td>Severe (3)</td>
<td>Major project objectives will not be realised, or there will be significant damage or loss to the University.</td>
</tr>
</tbody>
</table>

It may be appropriate to modify the indicated risks, their mitigating actions and/or the early warning signs as appropriate for your project.

Feel free to add extra rows to the table below for additional risks as required.

This template is available as a Microsoft Word document (which may be imported into OpenOffice.org if preferred).
<table>
<thead>
<tr>
<th>Description</th>
<th>P</th>
<th>I</th>
<th>Time</th>
<th>Response</th>
<th>Mitigation</th>
<th>Residual P/I</th>
<th>Early warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 There is a risk that the University is sued under the Data Protection Act 1998, due to inappropriate disclosure of personal information, failure to provide information to the data subject, an unauthorised transfer of personal data outside the European Economic Area or other breach, resulting in damage to reputation and financial loss.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See section 4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 There is a risk that the University is prosecuted under the Disability Discrimination Act 1995 or subsequent amendments, due to deficiencies in external service website accessibility, resulting in damage to reputation and financial loss.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See section 4.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 There is a risk that marks for student work are challenged by a student or an exam board, due to inadequate controls or audit trail on submitted work, resulting in wasted time and resources, possible financial loss, and damage to reputation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See section 4.3.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 There is a risk that unacceptable content is posted to and cannot be removed from a University-branded web service, resulting in legal action or damage to the University’s reputation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See sections 4.3.2, 4.3.3 and 4.1.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>P</td>
<td>I</td>
<td>Time</td>
<td>Response</td>
<td>Mitigation</td>
<td>Residual P/I</td>
<td>Early warning</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>There is a risk that the service supplier may cease trading or withdraw the service due to insolvency or other circumstances, resulting in the data stored on the service being unavailable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Plan and test a migration procedure for your data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that data stored in the service may become visible outside the group of people who are authorised to access it, due to service supplier error, to legal process, or to illegal access (hacking), resulting in violation of agreed confidentiality commitments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See section 4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that data entered into the system cannot be retrieved in a useful form, due to a lack of functionality or of standards, resulting in my data being “locked in” to the service.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Test the ability to extract data from the service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that the data is lost due to system failure and inadequate backup arrangements by the supplier, resulting in loss of vital information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Check supplier terms and conditions; ask about backup procedures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that the service becomes unusable or inaccessible due to performance problems at the supplier or in the Internet, resulting in delays or effective loss of service.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Check any discussion forums or mailing list archives for evidence of previous difficulties.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>P</td>
<td>I</td>
<td>Time</td>
<td>Response</td>
<td>Mitigation</td>
<td>Residual P/I</td>
<td>Early warning</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>There is a risk that the service is unavailable at crucial times due to planned downtime resulting in delays or waste of time and resources.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Ask supplier about planned downtime schedule and warning period.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that support from the service provider may not be available when needed due to time zone issues, resulting in delays or the temporary inability to use the service.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Investigate whether other support routes (e.g. user community support) are available and adequate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that the service may change in unexpected ways due to upgrades or business-related changes by the supplier, resulting in the service no longer being appropriate for your needs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Check supplier blogs for clues to future plans. Check industry news sources (e.g. TechCrunch) for rumours of changes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that the service provider may change its pricing due to business imperatives, resulting in an unexpected financial burden.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Check what pricing guarantees the supplier offers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that the data stored in the external service is lost due to a supplier deletion policy for apparently unused accounts, resulting in possible financial loss or damage to reputation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Check the terms and conditions for account deletion policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>P</td>
<td>I</td>
<td>Time</td>
<td>Response</td>
<td>Mitigation</td>
<td>Residual P/I</td>
<td>Early warning</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>For data of long-term value, there is a risk that the data cannot be preserved and used for as long as it is needed if the service provider is not committed to supporting the data through changes in data formats and standards.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Evaluate the supplier’s commitment to accepted technical standards and their record of responding to emerging standards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that the University becomes legally responsible for breaches of the Data Protection Act committed by the service provider because of the terms of the legal agreement, leaving the University open to being sued for things it did not do</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See section 4.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that users’ security is endangered due to lack of clarity as to what information will be publicly available.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See section 4.1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk that users are unclear as to what information they are giving to whom and for what purposes, leaving them exposed to unwanted communications or publication.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See section 4.1.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a risk of loss of intellectual property rights belonging to the users or the University as a result of the terms of service agreements.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Check the terms and conditions of service carefully and monitor them for any changes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>P</td>
<td>I</td>
<td>Time</td>
<td>Response</td>
<td>Mitigation</td>
<td>Residual P/I</td>
<td>Early warning</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>------</td>
<td>----------</td>
<td>----------------------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>20   There is a risk that users are exposed to unwanted marketing or spam because they are not told how to avoid these.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See section 4.1.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21   There is a risk that the service provider makes inappropriate use of cookies or tracking technologies to the detriment of users and the University.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See section 4.1.4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>