Information Services guidance on social networking

May 2011

Contents
1. Definitions .............................................................................................................................................. 2
2. Introduction ........................................................................................................................................... 3
3. IS and University Policy ...................................................................................................................... 3
   3.1 The IT Use Policy ............................................................................................................................ 3
   3.2 University Rules and Regulations .................................................................................................. 4
4. Post-breach ........................................................................................................................................... 5
   4.1 Inter-student communication ........................................................................................................... 5
   4.2 Student/Staff communication .......................................................................................................... 8
   4.3 Inter-staff communication .............................................................................................................. 10
   4.4 Third party complaints ................................................................................................................... 12
   4.5 Intellectual Property/Copyright Infringement .............................................................................. 13
5. Taking further steps ............................................................................................................................... 14
6. Evidence from IS for any disciplinary proceedings .......................................................................... 14
7. Prevention ............................................................................................................................................ 15
8. Conclusion ........................................................................................................................................... 15

Appendix A-Report a picture (Facebook) ............................................................................................... 17
Appendix B-Report/Block (Facebook) .................................................................................................... 17
Appendix C-Reporting a problem with Twitter ....................................................................................... 18
Appendix D- Social networking contact details .................................................................................... 19
   Facebook ............................................................................................................................................. 19
   Twitter ............................................................................................................................................... 19
Appendix E-Social networking terms and conditions of use .................................................................. 20
   Facebook ........................................................................................................................................... 20
   Twitter .............................................................................................................................................. 24
1. Definitions
In this document, the following words and phrases shall have the meaning ascribed to them below:

**University** means the University of Stirling;

**IT Use Policy** means the Information Technology Use Policy, including all Sections included within it;

**University Rules and Regulations** means the University Calendar Rules and Regulations, including all Sections included within it;

**Information Centre** means the information centre relating to information services at the University;

**Malicious Content** means information purposefully created and published in order to harm, discredit, or harass an individual or the University.

**Intellectual Property** means the output of intellectual endeavour in literary, artistic, dramatic, industrial, scientific and engineering fields, which is generally capable of being identified and protected. The protection of IP is provided through certain legal rights many of which are established under legislation, common law and international treaties;

**Social Networking Site** means ‘web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site’;¹

**Cyber-bullying** means ‘An aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself’.²

**Web2.0** means web applications and services that facilitate collaboration, user-centred designed, information sharing and interoperability.

**Facebook** means the social networking website [www.facebook.com](http://www.facebook.com). The most popular such site among staff and students at the University.³

**Twitter** means the social network website [www.twitter.com](http://www.twitter.com). Twitter is a ‘micro blogging’ tool enabling its users to send and receive small 140 character text messages.

---


³ The 2010 IS Satisfaction survey states that of the 1196 staff and students polled, 25.4% of staff and 29.5% of students use Facebook.
2. Introduction

The use of social networking tools such as Twitter, MySpace and Facebook have aided universities in gaining new audiences, promoting research, and creating new academic learning ‘spaces’. These new tools, however, have expanded the problems universities face with student discipline.

The tools may have changed, but the breaches of University rules and regulations remain the same as before the invention of web2.0 technologies. Before these technologies existed, students may have pinned up a poster defaming a lecturer, but now they need only make a post on a ‘virtual’ wall on Facebook. These student infractions are just variations on old themes presented in a new form.

To this end, it is fair to say that most disciplinary breaches using these new technologies are prohibited by existing applicable university policy or law and already have university procedures in place through the student rules and regulations or laws of defamation and copyright. The problem is not that there is a lack of specific University rules in place that govern these new technologies, but rather that students do not think that these existing rules relate to these web2.0 technologies. The real questions that face the University are, once the breach of conduct has occurred, what can be done by the University and how to start to prevent such breaches occurring in future?

3. IS and University Policy

As outlined in the introduction, the disciplinary cases regarding students’ use of social networking tools (old problem, new tools) appear to be already covered by the student rules and regulations and IT use policy, which include the following:

- Policy Statement on Harassment VI-63
- IT Use Policy-3.3 Prohibited use
- Intellectual Property Policy VI-78

3.1 The IT Use Policy

The definitions in section 1.4 of the IT Use Policy states that ‘Information’ is ‘any form of information or data capable of being stored or communicated in electronic form, including, without limitation, written, graphical, numerical, voice, music, video and multimedia data, Facebook (and similar social media) postings, YouTube material, Twitter postings, software and html and other programming code’. This blanket definition enables any malicious content posted on social networking sites to be classed as ‘information’ and therefore covered under section 3.3(a): Prohibited Use:

‘Information used by a User must not be offensive, abusive, discriminatory, illegal to possess, damage the University’s interests, or otherwise contravene University regulations. Users should note that possession or dissemination of such Information may be a criminal offence. Users should ensure that their Use of IT complies with all relevant UK and Scottish laws, including, without limitation, laws

4 Twitter, http://www.twitter.com
5 MySpace, http://www.myspace.com
6 Facebook, http://www.facebook.com
8 http://www.is.stir.ac.uk/docs/policy/itusepolicy.pdf
10 IT Use Policy, Section 1.4: http://www.is.stir.ac.uk/docs/policy/itusepolicy.pdf
relating to: discrimination on grounds of age, disability, gender reassignment, marriage and civil partnership status, pregnancy and maternity, sex, sexual orientation, race, religion and belief; libel and defamation; copyright protection. The University does not tolerate the use of its IT Systems to discriminate unlawfully, harass or bully.\textsuperscript{11}

Furthermore, the IT Use Policy explicitly states in 3.3(b) that the above statement ‘applies equally to all storage, processing or transmission of Information, examples of which would include viewing of web pages, data files and the content of emails, Facebook postings, Twitter postings, blogs, wikis, podcasts, Instant Messaging sessions and content produced by similar electronic communication tools and services’.\textsuperscript{12} This statement ensures that any malicious content posted to social networking sites are in breach of the University IT Use Policy.

3.2 University Rules and Regulations

The University Rules and Regulations cover a broad range of disciplinary infractions related to student conduct. These rules are not explicitly for social networking or indeed use of IT, however they can still be applied to students’ use of these technologies.

The University’s Policy Statement on Harassment VI-63, paragraph 2 states that:

‘No student or member of staff should:

i. be subjected to any form of harassment or bullying because of their race, disability, gender or sexual orientation;

ii. feel that such harassment has to be tolerated;

iii. feel that such harassment is his/her fault.’\textsuperscript{13}

This bullying policy clearly states that no harassment will be tolerated. In combination with the IT Use Policy outlined in section 3.1, it is recommended that no policy changes are required to govern any new web2.0 technologies that have emerged. The guidance stated in paragraph 13 of the Policy Statement on Harassment also provides a clear method (formal and informal) for dealing with any harassment complaint that may arise.

The University Intellectual Property Policy provides protection for the University with regards to any infringement on its IP. The policy states that the University own the IP created by staff members during their time at work. Students retain their own IP on any work they complete during their studies at the University. Paragraph 31 of the Intellectual Property Policy includes particular regulations for both staff and students to follow:

We respect the IP of others and expect our staff and students to. In particular:

- Staff and students may only use the IP of third parties in accordance with licences we have agreed with its owner(s).

\textsuperscript{11} IT Use Policy, Section 3.3(a) \url{http://www.is.stir.ac.uk/docs/policy/itusepolicy.pdf}
\textsuperscript{12} IT Use Policy, Section 3.3(b) \url{http://www.is.stir.ac.uk/docs/policy/itusepolicy.pdf}
\textsuperscript{13} Policy Statement on Harassment, VI-63, paragraph 2: \url{http://www.calendar.stir.ac.uk/documents/rules-and-regulations-policy-statement-on-harassment.pdf}
If staff or students wish to incorporate in their published work, teaching materials or assigned work material produced by others, responsibility will rest with them to establish and acknowledge the ownership of copyright of the material incorporated. They will be responsible for ensuring that any such incorporation from whatever source does not breach any relevant law and that appropriate Copyright Licensing Agency or other licences are not infringed. Such sources shall include, but are not restricted to, paper material, Internet and electronic mail sources, distance learning and other computer based materials, and graphical, musical and artistic materials.¹⁴

This paragraph outlines that staff and students must not infringe intellectual property law while at the University for work or study.

4. Post-breach
Breaches to the student rules and regulations and/or laws will inevitably occur using these new web2.0 technologies, and the reaction of the University will differ depending on the type of breach, and the social networking site involved. The two most popular social networking sites used by students at present are Facebook and Twitter and thus, guidance will be shown for these two sites.

Social networking disciplinary problems can be separated into five categories:

- Inter-student communication (‘cyber-bullying’, ‘profile spoofing/theft’ etc.)
- Student/staff communication (defamation, invasion of privacy, ‘cyber-stalking’ etc.)
- Inter-staff communication (staff members performing similar actions to that of Inter-student communication)
- 3rd party complaints about staff/students
- Intellectual Property/Copyright Infringement

It should be noted that all possible avenues for content removal should be explored before any consideration of legal action against the social networking provider. Legal action taken directly against students should only be taken as a very last resort, with the internal discipline procedure used for these cases.

4.1 Inter-student communication
The two most common forms that inter-student communication takes are ‘cyber-bullying’ and ‘profile spoofing’. Cyber-bullying, like ‘real-life’ bullying, is governed under the student rules and regulations. Cyber-bullying can be defined as “wilful and repeated harm inflicted through the medium of electronic text”¹⁵. Profile spoofing can be classed as a form of cyber bullying, and usually involves a user creating a social networking account in the name of the victim. The perpetrator then pretends to be the victim online, presenting the victim in a bad light. Once a spoof account is created, the perpetrator tends to use it to tarnish and discredit the victim in as many ways as possible, usually by stating false claims or by joining unpopular/illegal groups. In Scots Law, this is classed as defamation and in very extreme cases, legal action can be taken if required depending on the circumstances and the users involved (See Section 3: Taking further steps). Legal precedence in

England has already been established with the case of *Applause Store Productions Ltd and Firsht v Grant Raphael*; however no case has been tried in a Scottish court that relates to social networking and defamation.

The course of action to take varies depending on the social networking site involved:

### 4.1.1 Facebook

Out of all the social networking site, Facebook is the most popular among university students, and most used for cyber-bullying. Unfortunately it is one of the most difficult sites to find guidance and report infringing items. It is also the most inconsistent site for removal of content after a report has been filed. To ensure that as much evidence is taken for any disciplinary cases, students can be advised to do the following:

1. **Gather evidence:** students should take printed and electronic copies of any correspondence that amounts to bullying. Electronic copies can be created by using the ‘print screen’ button on their keyboard and pasting the subsequent image into a document in Microsoft Word. Every item of Facebook content has a unique URL (web address). Students should always record these URLs. If any assistance is required, Information Services can assist in recording the evidence.

2. **Contact the Information Centre** (information.centre@stir.ac.uk) so that the University’s usage records can be checked for evidence. Give specific dates, times and websites (Facebook, Twitter etc.) for when the content was meant to have been posted.

3. **Once evidence has been gathered,** the student must report the malicious content to Facebook themselves. This can be done by using the ‘report’ links on Facebook. Depending on the situation, the report link can be in different places:
   a. **Photograph:** there will be a ‘report this photo’ link on the page for the particular photo (see Appendix A) and choose the most appropriate option, usually ‘Attacks individuals or group’.
   b. **Direct message:** there will be a ‘report’ link next to the senders name on the message. However be aware that the ‘report’ link only appears if the sender is not a ‘friend’ of victim.
   c. **Any other abuse (status updates, profile spoofing/stealing etc.):** there will be a ‘report/block this person’ link in the bottom left of the profile page for the user. Clicking on this will reveal many options for reporting the profile including ‘cyber bullying’ and ‘fake profile’ in which you can enter further details (see Appendix B).

Members of staff are able to report directly malicious content but this will be depend on the level of privacy set on the content in question, however Facebook state that you need to be a registered Facebook user to file a report. The first steps should always be to demonstrate to the student how to report the content themselves as this will be the quickest resolution for removal of the content. The easiest ‘blanket’ method to report any malicious content as a member of staff is to complete the ‘Report a violation of Facebook’s Terms of Use’ (which is very well hidden by Facebook as they want all users to register with them before reporting anything).

---

16 *Applause Store Productions Ltd and Firsht v Grant Raphael* [2008] EWHC 1781 (QB)

If content is set to ‘private’ or ‘friends only’, it may be difficult for members of staff (even if they have a Facebook profile) to view the content in question. If the student has recorded the URL of the malicious content, the URL can be used in the above ‘Report a violation’ contact form.

4. If the content is not removed by Facebook in a timely manner, further action can be taken (See section 3: Taking further steps, although in most cases, students would have to seek legal guidance as it is an individual’s problem rather than a University or University staff problem). Legally proving a student was 100% involved with the malicious content is a lengthy and costly procedure (see Section 4: Evidence from IS for any disciplinary proceedings), however this would not be required for an internal disciplinary procedure.

4.1.2 Twitter
Twitter, although much younger than Facebook, has grown to become one of the most popular web2.0 technologies. Unlike Facebook, which can contain many different types of rich media, and many ways to breach the student rules and regulations, Twitter is ‘text-only’ and allows users only 140 characters to express themselves. However, Twitter seems much more relaxed with their view on cyber bullying stating that “Twitter provides an open platform for its users to express a broad spectrum of views. We do not moderate the content provided by our users; users are solely responsible for the content that they provide”\(^\text{18}\). Twitter also suggests that reports can only be filed when there are specific violent threats; however it is still worth reporting any non-violent content.

The simpler delivery method of Twitter, coupled with a much clearer and simpler reporting mechanism, ensures that reporting content is much easier than Facebook:

1. Gather evidence: As with Facebook, you can take screenshots of any malicious Twitter postings and paste them into word processing software. To view an individual tweet in order to capture it for evidence, click on the date and time below the tweet to view the single tweet on a page on its own.
2. Contact the Information Centre (information.centre@stir.ac.uk) so that the University’s usage records can be checked for evidence. Give specific dates, times and websites (Facebook, Twitter etc.) for when the content was meant to have been posted.
3. Twitter make reporting any content very easy. In order to report something, the user must create a new support ticket\(^\text{19}\). The options to take are as follows (see Appendix C for an illustration of this):
   a. **Dear Twitter:** “I have a bone to pick with you”.
   b. **Subject:** enter a suitable subject.
   c. **Regarding:** Impersonation” or “Violent threat, harassment”
   d. **Sharing is caring:** Include as much details as possible including the student name, address, phone number, and any direct links to the content that you wish to be removed (use the direct URL to the single tweet if possible). If you need to upload any supportive documents, use the University file drop facility\(^\text{20}\) and link to the file.

---


\(^\text{19}\) [http://help.twitter.com/requests/new](http://help.twitter.com/requests/new)

\(^\text{20}\) [https://extranet.stir.ac.uk/drop/](https://extranet.stir.ac.uk/drop/)
Twitter states that only the user directly affected can report content “or a party legally authorized to act on their behalf”. Due to this, members of staff can only offer guidance to the student with regards how to report malicious content to Twitter.

4. If the content posted on Twitter is not a violent threat or impersonation, Twitter may reply that they are not responsible for the content posted by their users. This can be pursued by legal channels, however it is worth noting that unlike Facebook, Twitter is a fluid, time-sequenced technology which means that any comment posted will eventually ‘drop down’ the list of Tweets posted and will become unseen by most people (the yesterdays news/chip wrapper analogy applies here). Due to this, single breaches may not be worth pursuing, but long-running campaigns of bullying would still be worth closer examination. Again, with Facebook, exact proof of who posted the malicious content can be difficult to acquire (see section 4: Evidence from IS for any disciplinary proceedings).

4.2 Student/Staff communication
This area of communication is a key problem at universities and the most common problem is that of defamation. In Scots law, defamation is defined as:

“To be actionable, a defamatory statement must be false and able to "lower the plaintiff in the estimation of right-thinking members of society".”

In a university context, these tend to be students making ill-judged comments regarding their lecturers or tutors on Facebook or Twitter, or more seriously, creating Facebook groups that defame a member of staff and invite other students to do the same. Similar steps to that of student/student communication need to be taken:

4.2.1 Facebook

1. Gather evidence: staff should take printed and electronic copies of any malicious content or profile spoofing activity. Electronic copies can be created by using the ‘print scrn’ button on their keyboard and pasting the subsequent image into a document in Microsoft Word. Every item of Facebook content has a unique URL (web address). Staff should always record these URLs. If any assistance is required, Information Services can assist in recording the evidence.

2. Contact the Information Centre (information.centre@stir.ac.uk) so that the University’s usage records can be checked for evidence. Give specific dates, times and websites (Facebook, Twitter etc.) for when the content was meant to have been posted.

---


22 Sim v Stretch [1936] 2 All England Law Reports 1237 per Lord Atkin at p. 1240, although an English case, the test has been held as applicable to Scots law also, see Steele v Scottish Daily Record and Sunday Mail 1970 Scots Law Times S3.
3. Once evidence has been gathered, the member of staff must report the malicious content to Facebook themselves in the first instance. This can be done by using the ‘report’ links on Facebook. Depending on the situation, the report link can be in different places:
   a. **Photograph:** there will be a ‘report this photo’ link on the page for the particular photo (see Appendix A) and choose the most appropriate option, usually ‘Attacks individuals or group’.
   b. **Direct message:** there will be a ‘report’ link next to the senders name on the message. However be aware that the ‘report’ link only appears if the sender is not a ‘friend’ of victim.
   c. **Groups:** there will be a ‘report group’ link in the bottom left of the group page enabling you to report the group. The usual reason to enter in the subsequent box is ‘targets me or a friend’ and then enter the location of where the abuse occurred within the group. If it’s the entire group that is malicious, choose the ‘title’ option.
   d. **Any other abuse (status updates, profile spoofing/stealing etc.):** there will be a ‘report/block this person’ link in the bottom left of the profile page for the user. Clicking on this will reveal many options for reporting the profile including ‘cyber bullying’ and ‘fake profile’ in which you can enter further details (see Appendix B).

As with student/student interaction, a member of staff can submit a generic ‘Terms of Service Violation’ form in which they can explain exactly what they wish to remove. The University may be able to act on behalf of the member of staff in requesting any content to be removed by filling in the violation form; however it is quicker for the member of staff to report it in the first instance.

4. If the content is not removed by Facebook in a timely manner, further action can be taken (See section 3: Taking further steps) by the University in order to request for the content to be removed. It also may be worth repeating the reporting of content as the University rather than the individual member of staff.

Legally proving a student 100% was involved with the malicious content is a lengthy and costly procedure (see Section 4: Evidence from IS for any disciplinary proceedings), however this would not be required for an internal disciplinary procedure.

### 4.2.2 Twitter

As outlined in section 2.1.2, Twitter states “Twitter provides an open platform for its users to express a broad spectrum of views. We do not moderate the content provided by our users; users are solely responsible for the content that they provide”. This seems to include any defamatory statement created on Twitter. Unless the tweet contains any direct threat of violence, impersonation, or copyright infringement they will probably not remove the malicious content (although it is worth trying). Twitter appears to want to leave any defamatory content up, with the responsibility being on the user who placed it there in the first place to remove it.

In order to petition Twitter to remove any tweets:

1. Gather evidence: As with Facebook, you can take screenshots of any malicious Twitter postings and paste them into word processing software. To view an individual tweet in order to capture it for evidence, click on the date and time below the tweet to view the single tweet on a page on its own.

2. Contact the Information Centre (information.centre@stir.ac.uk) so that the University’s usage records can be checked for evidence. Give specific dates, times and websites (Facebook, Twitter etc.) for when the content was meant to have been posted.

3. Twitter make reporting any content very easy. In order to report something, the user must create a new support ticket\(^\text{24}\). The options to take are as follows (see Appendix C for an illustration of this):
   a. **Dear Twitter:** “I have a bone to pick with you”.
   b. **Subject:** enter a suitable subject.
   c. **Regarding:** “Impersonation” or “Violent threat, harassment”
   d. **Sharing is caring**: Include as much details as possible including the student name, address, phone number, and any direct links to the content that you wish to be removed (use the direct URL to the single tweet if possible). If you need to upload any supportive documents, use the University file drop facility\(^\text{25}\) and link to the file.

   Twitter states that only the user directly affected can report content “or a party legally authorized to act on their behalf”. In certain cases, the University legal team may be able to act on behalf of a member of staff, but in the first instance, the member of staff should report the malicious content themselves (with help and guidance from the University).

4. If the content posted on twitter is not a violent threat or impersonation, Twitter may reply that they are not responsible for the content posted by their users. This can be pursued by legal channels (see section 3: Taking further steps), however it is worth noting that unlike Facebook, Twitter is a fluid, time-sequenced technology which means that any comment posted will eventually ‘drop down’ the list of Tweets posted and will become unseen by most people (the yesterdays news/chip wrapper analogy springs to mind). Due to this, single breaches may not be worth pursuing, but long-running campaigns of bullying would still be worth pursuing. Again, with Facebook, exact proof of who posted the malicious content can be difficult to acquire (see section 3: Evidence from IS for any disciplinary proceedings).

### 4.3 Inter-staff communication
Staff communication on social networking should be encouraged in most cases; it can build academic relationships, create new techniques for learning and research, and promote the University across the world. However it also can prove to be a problematic tool for the University; staff members must be careful in how they conduct themselves online, manage their privacy, and represent the University in the best possible way.

\(^{24}\) [http://help.twitter.com/requests/new](http://help.twitter.com/requests/new)

\(^{25}\) [https://extranet.stir.ac.uk/drop/](https://extranet.stir.ac.uk/drop/)
For both Facebook and Twitter, the techniques for reporting malicious content by staff are the same as outlined in sections 4.1.1 and 4.1.2 for students, however, as staff members are employed to represent the University, guidelines should be in place in order to help staff best represent their own, and the University’s, interests. The guidelines can be split into two clear categories: officially representing the University on social networks, and unofficially representing the University through staff members own personal interactions.

4.3.1 Official interactions

Official interactions occur through the creation of social networking profiles and subsequent interactions on behalf of the University and/or departments. The following guidelines should be followed in order to ensure that the University is represented accurately and fairly at all times:

- **Follow the rules**-members of staff should always be mindful of the terms and conditions of the social networking site, and the University IT Use Policy.

- **Transparency**-the member of staff should clearly state who they are and always state their affiliation to the University. If the members of staffs’ interactions are regarding the University, always acknowledge your relationship to the University.

- **Confidentiality**-members of staff should never disclose confidential information on social networking sites. This includes any non-public financial information, and any information related to the non-public strategies, policies and management decisions. Personal information about members of staff or students should never be disclosed.

- **Accuracy**- members of staff should take all reasonable steps that the information shared is accurate. If members of staff have been asked a question and they are unsure of the answer, they should respond that they will find out the answer, rather than risking giving possible incorrect information. It can be incredibly difficult to correct work information on a social networking site, especially as it may have been re-communicated virally.

- **Respect**-members of staff should always respect the community when communicating on social networks. They should never abuse the community and always ‘think before acting’ when communicating.

- **Personal views**-members of staff should always remember they are posting on behalf of the University and should always uphold the University’s mission and values. Do not include comments on political or social issues unless they are in support of the University’s positions on these issues.

- **Resources**-members of staff should never start social networking interaction (for example creating a new Twitter profile) if they do not have the resources for a sustainable long-term approach.

- **Feedback**-social networking sites are excellent tools for receiving feedback. If staff members participate in any social networking, they must be prepared to accept negative feedback, and also be prepared to act on any feedback that they receive.

4.3.2 Unofficial interactions

A large proportion of staff members already use social networking in the context of their personal and home life. Unofficial interaction relates to the presentation and image the member of staff is projecting on such sites. Although this interaction is unrelated directly to the University, members of staff must be mindful of how their actions on such sites can affect the University and should never engage in activities that might bring the University into disrepute:
• **Privacy**-members of staff should ensure that their social networking profiles have the relevant privacy settings to ensure that only authorised users can view their information. Members of staff should not provide more personal information than required such as personal and work contact details.

• **Honesty**-members of staff can identify themselves as working for the University. However if they are sharing any views or comments, they must be clear they are doing so as a member of the higher education community (or an individual), not as a formal representative of the University. The External Relations department will be able to assist with any formal statements that members of staff wish to make regarding their identity.

• **Perception**-As the use of social networking explodes, the lines between personal and professional, public and private blur further. If a member of staff identifies themselves as working for the University, they are creating a perception about the University, its students, staff, and customers. Members of staff should always be aware that content associated with them is a fair representation of themselves and the University. Content can be protected to some extent using privacy features, but nothing on internet is truly private, and as such members of staff should never post content that will bring themselves, or the University, into disrepute.

• **Impersonation**-members of staff should never impersonate any other person while using social networking sites. Members of staff should never create social networking content about the University and not disclose their affiliation (for example pretending to be an external user to promote the University). With the advancements in social networking technology, this abuse can be easily traced to the University member of staff and may directly lead to branding, image, and media problems for the University.

• **Respect**-members of staff should always respect the community when communicating on social networks. They should never abuse the community and always ‘think before acting’ when communicating.

• **Liability**-members of staff must be aware they are legally liable for any content posting on social networking sites and may be challenged legally if the content is deemed to be proprietary, copyrighted, defamatory, or obscene.

• **Respect University time and property**-Personal social networking should only be used by members of staff at work in accordance with the Private Use of IT section within the Information Services IT Use Policy. This states ‘for staff, such private Use does not interfere with their individual work as an employee or impede the work of other Users;’ ²⁶ and ‘the private Use must not involve activities which may bring the University into disrepute or which involve a misstatement implying that such Use is official Use in accordance with University business or otherwise not in a private capacity;’ ²⁷

4.4 Third party complaints
Complaints regarding staff or student conduct on social networking sites can be received by the University. The largest percentage of such complaints relate to Intellectual Property infringement, harassment and defamation. The University’s response will vary depending on the specific infractions of the University Rules and Regulations and IT Use Policy. If a third party complaint is received regarding malicious content posted on social networking sites, the University must explain

²⁶ IT Use Policy, Section 3.2(b ii): [http://www.is.stir.ac.uk/docs/policy/itusepolicy.pdf](http://www.is.stir.ac.uk/docs/policy/itusepolicy.pdf)
²⁷ IT Use Policy, Section 3.2(b vii) : [http://www.is.stir.ac.uk/docs/policy/itusepolicy.pdf](http://www.is.stir.ac.uk/docs/policy/itusepolicy.pdf)
to the third party the process of reporting the content in order to expedite its removal (in most cases the content will be removed quicker if the victim reports it). Evidence should be kept of the malicious content in case any action under the University disciplinary procedures is to proceed. The University may also act as an intermediary and contact the staff/student directly to request the content is removed.

If the content was posted using a personal social networking account (i.e. a non-sanctioned official University profile), any legal challenges to the content will have to be dealt with by the individual staff/student responsible rather than the University.

4.5 Intellectual Property/Copyright Infringement

Compared with other infractions, Copyright Infringement (CI) appears to be high priority among social networking sites. All sites appear to have clear CI policies and procedures to deal with any infringement that may occur. Within a university setting, CI and infringements on a person’s intellectual property can range from a student posting material from a lecture through to doctoring a photograph of a member of staff.

The following simple steps need to be completed in order for material to be removed:

4.5.1 Facebook

Facebook has two separate forms that the copyright or intellectual property holder must complete in order for Facebook to remove the offending items:

1. Copyright Infringement:
   http://www.facebook.com/legal/copyright.php?copyright_notice=1&type=1&uid=0&cid=8284540812&cid2=0&h=583bc6fee7

2. Intellectual Property Infringement:
   http://www.facebook.com/legal/copyright.php?noncopyright_notice=1&type=1&uid=0&cid=8284540812&cid2=0&h=583bc6fee7

4.5.2 Twitter

You can report a CI to Twitter via emailing copyright@twitter.com with the following details:

- A physical or electronic signature of the copyright owner or a person authorized to act on their behalf;
- Identification of the copyrighted work claimed to have been infringed;
- Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit us to locate the material;
- Your contact information, including your address, telephone number, and an email address;
- A statement by you that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and
- A statement that the information in the notification is accurate, and, under penalty of perjury, that you are authorized to act on behalf of the copyright owner.
5. Taking further steps
If the steps in Section 4 fail to remove items from the indicated social networking sites, in the first instance, the best course of action would be to repeat the request for the content to be removed by either the individual or as the University. If this is ignored again, further action through the University legal team can be investigated. However this would be mostly for cases of staff/student interaction and copyright. Student/student communication in most cases could not be taken on by the University as it is the responsibility of the students to take further legal action. In the first instance, a letter to the social networking site (details in Appendix E) from the University lawyers asking for the removal of the content within a stated timeframe would suffice. These combined actions should result in the very large majority of any requested content being removed. If this is not adhered to, further legal action can be taken, however this can be an expensive undertaking.

Individuals (for example staff/students) can take legal action against the perpetrator of the malicious content to seek damages. This depends on the circumstances (mostly in relation to copyright infringement or defamation of character), however defamation legal action is a very last resort and student disciplinary action should be sufficient for the all but the most serious cases (there may be large university PR implications for any staff member suing a student for defamation).

6. Evidence from IS for any disciplinary proceedings
A problem with social networking sites is that without legal interference it is impossible to receive further details from the social networking site regarding the exact IP address of the computer that was used to perform the malicious action, and thus trace back to prove it was the University user in question (this only applies if they were connected to Campusnet or using a campus computer). The other problem is that with the explosion in mobile device use, students may not connect through the university to the social networks, but rather they may use their mobile device (IPhone, Blackberry etc.). If mobile devices were used, further legal action would have to be taken with the mobile provider to prove that the IP address received from the social networking site was used by the mobile device of the student who is being disciplined.

If the student used the university network to use these social networking sites for malicious reasons, the logs on the university’s web activity logs can be checked. These can prove that the student was connected to a certain website at a certain time. There are two problems however: the first is that the activity logs are only kept for five days, so speed is essential in reporting any malicious actions. The second problem is that although the logs can confirm that the student was on a particular website at a particular time, it cannot prove the content of what was being posted by the student, and thus, it cannot be proven 100% that a student posted any malicious content (it could be legally argued that it was coincidence that the student was online at that time while someone else pretended to be that student and posted malicious content). These issues may be problematic in any legal proceedings, however for university disciplinary action, the logs from the University servers can be used as evidence. Contact the Information Centre (informationcentre@stir.ac.uk) in the first instance to ask for the server logs to be checked. In order for the logs to be checked, certain information will be needed including: registration number or user name of the student (in order for the Information Centre to find their computer account username) and the date/times and site of the malicious content.
7. Prevention
Student education and prevention is important in tackling these types of problems in the long term. A ‘light touch’ approach is required at all times however, and education should be performed in the students’ best interests rather than the University.28

A proven technique in persuading students to ‘think before they act’ is to inform them that in these digital times, they must think carefully about how they wish to ‘brand’ themselves online. With potential employers (and even students’ parents!) searching for information about the student, they must be careful about their online image.

To tackle student’s behaviour online, and implement the above technique, it would be beneficial to include a slide and a couple of minutes of talk time in the new student inductions. This would outline the above statement regarding how they want to appear online, and could also cover some simple ‘dos and don’ts’ on social networks in an academic setting. This also covers any problems when the student claims that they ‘did not know’ if they are then disciplined for a social network problem. It is also worth noting to the students that they can use social networks to great affect in their academic lives as a positive communication tool between staff and students.

To aid staff and students across the University, this document can be used as a basis for creating short ‘fact sheets’ that can then be used for guidance for social networking. Examples of such sheets could include:

- Advice for students on conducting themselves on social networks.
- Advice for staff on representing the University and conducting themselves on social networks.
- Advice for staff and students if they are the victim of any malicious content on social networks.
- Advice for ‘front line’ staff (Residential Services/Information Centre) and line managers on how to aid students or staff with social networking complaints.

8. Conclusion
Social networking and other web2.0 tools and services are important and relevant technologies that the University should embrace to support research, learning and teaching. However, these new tools have created a new frontier for a very old problem. Disciplinary cases regarding student bullying, harassment, and even students targeting lecturers have been around since the formation of this University. As a whole, the student rules and regulations and IT use policy hold up well in addressing any specific disciplinary problems that arise from these technologies, however, the tools for researching and evidence gathering are wholly different than anything before. Even with studying just two of the plethora of social networking tools available, it can be seen that they have vastly different methods of reporting malicious content and its subsequent removal. If the social networking sites fail to remove content, then legal action can be considered by the University in order to get the content removed. Legal action against any individuals involved in these cases is a very last resort as the large majority of all cases will involve University students who can be

28 In 2007, Keele University emailed all students asking them to never write anything derogatory about their university on social networking sites. This did not sit well with students who felt their freedom of speech was being violated: [http://www.theregister.co.uk/2007/05/22/keele_facebook/](http://www.theregister.co.uk/2007/05/22/keele_facebook/).
disciplined via the internal disciplinary procedure. Any legal action should be carefully considered before any action is taken as this may affect the University and have larger PR implications.

In order to prevent these infringements from occurring in future, education is a key tool in informing students of the benefits and risks associated with social networking in a higher education context and should be used to try and reduce the number of future incidents.
Appendix A-Report a picture (Facebook)

Report a Picture

You are about to report a violation of our Terms of Use. All reports are strictly confidential.

We will NOT remove photos just because they're unflattering.

Reason: 
(required)  Attacks individual or group

Facebook removes photos for attacking an individual or group if:

- the photo has been edited to attack an individual or group
- the caption or tags attack an individual or group
- the image is hateful or racially, ethnically or otherwise objectionable

Facebook will not remove a photo for attacking an individual or group if:

- the photo is simply unflattering
- the individual pictured does not like the way they look
- the photo does not violate our Terms of Use

I have reviewed the Terms of Use and the above guidelines, and I certify that the content I am reporting violates Facebook's abuse standards. I understand that blatant or repeated invalid reports could result in disciplinary action being taken against my account.

Is this your intellectual property?  
Submit  Cancel

Appendix B-Report/Block (Facebook)

Report and/or block

You are about to report a violation of our Terms of Use. All reports are strictly confidential.

If you are reporting someone for an inappropriate group, message, post, etc., please do so through the report link on the page where you see that content.

Block this person

If you block someone, they will not be able to find you in a Facebook search, see your profile, or interact with you through Facebook channels (such as Wall posts, Poke, etc.). Any Facebook ties you currently have with a person you block will be broken (for example, friendship connections, relationship status, etc.). Note that blocking someone may not prevent all communications and interactions in third-party applications, and does not extend to elsewhere on the Internet.

Report this person

Reason: 
(required)  Fake profile

Report type: 
(required)  Impersonating me or someone else

Impersonated profile: 
(required)  http://www.facebook.com/profile.php?id=xxx

Is this your intellectual property?  
Submit  Cancel
Appendix C-Reporting a problem with Twitter

Submit a request

Dear Twitter,*

I have a bone to pick with you

Regarding *

Impersonation

Sharing is caring! *
Fill in the details of your request here. Include user names, links to relevant tweets or screen shots, and steps to reproduce the problem, when applicable. For security reasons, we do not accept attachments.

Check the Known Issues pages, @twitter, or the Status Blog for updates on problems.

Love, (Enter your Twitter user name here) *

Please enter your email address *

Tell us more

Using your phone with Twitter? Enter the number here:

I feel:

Submit
Appendix D- Social networking contact details

Facebook
Facebook, Inc
1601 S. California Avenue
Palo Alto, CA 94304
USA

Twitter
Twitter, Inc.
Attn: Copyright Agent
795 Folsom Street, Suite 600
San Francisco, CA 94103
USA
Appendix E-Social networking terms and conditions of use

Relevant terms of use are highlighted in bold and underlined.

Facebook

This agreement was written in English (US). Please note that Section 16 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: April 22, 2010

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement") derives from the Facebook Principles, and governs our relationship with users and others who interact with Facebook. By using or accessing Facebook, you agree to this Statement.

1. Privacy

Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions.

2. Sharing Your Content and Information

You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

1. For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.

2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).

3. When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Privacy Policy and About Platform page.)

4. When you publish content or information using the "everyone" setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).

5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

3. Safety

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to do that, which includes the following commitments:

1. You will not send or otherwise post unauthorized commercial communications (such as spam) on Facebook.

2. You will not collect users’ content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.

3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.

4. You will not upload viruses or other malicious code.

5. You will not solicit login information or access an account belonging to someone else.

6. You will not bully, intimidate, or harass any user.

7. You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.

8. You will not develop or operate a third-party application containing alcohol-related or other mature content (including advertisements) without appropriate age-based restrictions.

9. You will not offer any contest, giveaway, or sweepstakes ("promotion") on Facebook without our prior written consent. If we consent, you take full responsibility for the promotion, and will follow our Promotions Guidelines and all applicable laws.

10. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.

11. You will not do anything that could disable, overburden, or impair the proper working of Facebook, such as a denial of service attack.

12. You will not facilitate or encourage any violations of this Statement.

4. Registration and Account Security
Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal profile.
3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal profile for your own commercial gain (such as selling your status update to an advertiser).
5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password, (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any page or application you administer) to anyone without first getting our written permission.
10. If you select a username for your account we reserve the right to remove or reclaim it if we believe appropriate (such as when a trademark owner complains about a username that does not closely relate to a user’s actual name).

5. Protecting Other People’s Rights

We respect other people’s rights, and expect you to do the same.

1. You will not post content or take any action on Facebook that infringes or violates someone else’s rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement.
3. We will provide you with tools to help you protect your intellectual property rights. To learn more, visit our How to Report Claims of Intellectual Property Infringement page.
4. If we remove your content for infringing someone else’s copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
5. If you repeatedly infringe other people’s intellectual property rights, we will disable your account when appropriate.
6. You will not use our copyrights or trademarks (including Facebook, the Facebook and F Logos, FB, Face, Poke, Walls and 32665), or any confusingly similar marks, without our written permission.
7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
8. You will not post anyone’s identification documents or sensitive financial information on Facebook.
9. You will not tag users or send email invitations to non-users without their consent.

6. Mobile

1. We currently provide our mobile services for free, but please be aware that your carrier’s normal rates and fees, such as text messaging fees, will still apply.
2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are not sent to the person who acquires your old number.
3. You provide all rights necessary to enable users to sync (including through an application) their contact lists with any basic information and contact information that is visible to them on Facebook, as well as your name and profile picture.

7. Payments

If you make a payment on Facebook or use Facebook Credits, you agree to our Payments Terms.

8. Special Provisions Applicable to Share Links

If you include our Share Link button on your website, the following additional terms apply to you:

1. We give you permission to use Facebook’s Share Link button so that users can post links or content from your website on Facebook.
2. You give us permission to use and allow others to use such links and content on Facebook.
3. You will not place a Share Link button on any page containing content that would violate this Statement if posted on Facebook.

9. Special Provisions Applicable to Developers/Operators of Applications and Websites

If you are a developer or operator of a Platform application or website, the following additional terms apply to you:

1. You are responsible for your application and its content and all uses you make of Platform. This includes ensuring your application or use of Platform meets our Developer Principles and Policies and our Advertising Guidelines.
2. Your access to and use of data you receive from Facebook, will be limited as follows:
   1. You will only request data you need to operate your application.
   2. You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data.
   3. You will not use, display, share, or transfer a user’s data in a manner inconsistent with your privacy policy.
   4. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide a mechanism for users to make such a request.
   5. You will not include data you receive from us concerning a user in any advertising creative.
   6. You will not directly or indirectly transfer any data you receive from us to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use.
7. We can limit your access to data.
8. You will comply with all other restrictions contained in our Developer Principles and Policies.
9. You will not give us information that you independently collect from a user or a user’s content without that user’s consent.
10. You will make it easy for users to remove or disconnect from your application.
11. You will not make it easy for users to contact you. We can also share your email address with users and others claiming that you have infringed or otherwise violated their rights.
12. You will provide customer support for your application.
13. You will not show third party ads or web search boxes on Facebook.
14. We will give you all rights necessary to use the code, APIs, data, and tools you receive from us.
15. You will not sell, transfer, or sublicense our code, APIs, or tools to anyone.
16. You will not misrepresent your relationship with Facebook to others.
17. You may use the logos we make available to developers or issue a press release or other public statement so long as you follow our Developer Principles and Policies.
18. We can issue a press release describing our relationship with you.
19. You will comply with all applicable laws. In particular you will (if applicable):
   1. have a policy for removing infringing content and terminating repeat infringers that complies with the Digital Millennium Copyright Act.
   2. comply with the Video Privacy Protection Act ("VPPA"), and obtain any opt-in consent necessary from users so that user data subject to the VPPA may be shared on Facebook. You represent that any disclosure to us will not be incidental to the ordinary course of your business.
20. We do not guarantee that Platform will always be free.
21. You will give us all rights necessary to enable your application to work with Facebook, including the right to incorporate content and information you provide to us into streams, profiles, and user action stories.
22. You give us the right to link to or frame your application, and place content, including ads, around your application.
23. We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search).
24. To ensure your application is safe for users, we can audit it.
25. We can create applications that offer similar features and services to, or otherwise compete with, your application.

10. About Advertisements on Facebook

Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you. In order to do that, you agree to the following:

1. You can use your privacy settings to limit how your name and profile picture may be associated with commercial or sponsored content served by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.
2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

11. Special Provisions Applicable to Advertisers

You can target your specific audience by buying ads on Facebook or our publisher network. The following additional terms apply to you if you place an order through our online advertising portal ("Order"):  
1. When you place an Order, you will tell us the type of advertising you want to buy, the amount you want to spend, and your bid. If we accept your Order, we will deliver your ads as inventory becomes available.
2. You will pay for your Orders in accordance with our Payments Terms. The amount you owe will be calculated based on our tracking mechanisms.
3. Your ads will comply with our Advertising Guidelines.
4. We will determine the size, placement, and positioning of your ads.
5. We do not guarantee the activity that your ads will receive, such as the number of clicks you will get.
6. We cannot control how people interact with your ads, and are not responsible for click fraud or other improper actions that affect the cost of running ads. We do, however, have systems to detect and filter certain suspicious activity, learn more here.
7. You can cancel your Order at any time through our online portal, but it may take up to 24 hours before the ad stops running. You are responsible for paying for those ads.
8. Our license to run your ad will end when we have completed your Order. You understand, however, that if users have interacted with your ad, your ad may remain until the users delete it.
9. We can use your ads and related content and information for marketing or promotional purposes.
10. You will not issue any press release or make public statements about your relationship with Facebook without written permission.
11. We may reject or remove any ad for any reason.

If you are placing ads on someone else's behalf, we need to make sure you have permission to place those ads, including the following:

12. You warrant that you have the legal authority to bind the advertiser to this Statement.
13. You agree that if the advertiser you represent violates this Statement, we may hold you responsible for that violation.

12. Special Provisions Applicable to Pages

If you create or administer a Page on Facebook, you agree to our Pages Terms.

13. Amendments
1. We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page) and an opportunity to comment. To get notice of any future changes to this Statement, visit our Facebook Site Governance Page and become a fan.

2. For changes to sections 7, 8, 9, and 11 (sections relating to payments, application developers, website operators, and advertisers), we will give you a minimum of three days notice. For all other changes we will give you a minimum of seven days notice. All such comments must be made on the Facebook Site Governance Page.

3. If more than 7,000 users comment on the proposed change, we will also give you the opportunity to participate in a vote in which you will be provided alternatives. The vote shall be binding on us if more than 30% of all active registered users as of the date of the notice vote.

4. We can make changes for legal or administrative reasons, or to correct an inaccurate statement, upon notice without opportunity to comment.

14. Termination

If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13, and 14-18.

15. Disputes

1. You will resolve any claim, cause of action or dispute (“claim”) you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.

2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim.

3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL BE SAFE OR SECURE. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: "A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR." WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

16. Special Provisions Applicable to Users Outside the United States

We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users outside the United States:

1. You consent to having your personal data transferred to and processed in the United States.

2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department’s list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website.

3. Certain specific terms that apply only for German users are available here.

17. Definitions

1. By "Facebook" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; and (c) other media, software (such as a toolbar), devices, or networks now existing or later developed.

2. By "us," "we" and "our" we mean Facebook, Inc., or if you are outside of the United States, Facebook Ireland Limited.

3. By "Platform" we mean a set of APIs and services that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.

4. By "information" we mean facts and other information about you, including actions you take.

5. By "content" we mean anything you post on Facebook that would not be included in the definition of "information."

6. By "data" we mean content and information that third parties can retrieve from Facebook or provide to Facebook through Platform.

7. By "post" we mean post on Facebook or otherwise make available to us (such as by using an application).

8. By "use" we mean use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.

9. By "active registered user" we mean a user who has logged into Facebook at least once in the previous 30 days.
10. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives data from us.

18. Other

1. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
2. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
3. If we fail to enforce any of this Statement, it will not be considered a waiver.
4. Any amendment to or waiver of this Statement must be made in writing and signed by us.
5. You will not transfer any of your rights or obligations under this Statement to anyone else without our consent.
6. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
7. Nothing in this Statement shall prevent us from complying with the law.
8. This Statement does not confer any third party beneficiary rights.

Twitter

These Terms of Service ("Terms") govern your access to and use of the services and Twitter’s websites (the “Services”), and any information, text, graphics, or other materials uploaded, downloaded or appearing on the Services (collectively referred to as “Content”). Your access to and use of the Services is conditioned on your acceptance of and compliance with these Terms. By accessing or using the Services you agree to be bound by these Terms.

Basic Terms

You are responsible for your use of the Services, for any content you post to the Services, and for any consequences thereof. The Content you submit, post, or display will be able to be viewed by other users of the Services and through third party services and websites (go to the account settings page to control who sees your Content). You should only provide Content that you are comfortable sharing with others under these Terms.

You may use the Services only if you can form a binding contract with Twitter and are not a person barred from receiving services under the laws of the United States or other applicable jurisdiction. You may use the Services only in compliance with these Terms and all applicable local, state, national, and international laws, rules and regulations.

The Services that Twitter provides are always evolving and the form and nature of the Services that Twitter provides may change from time to time without prior notice to you. In addition, Twitter may stop (permanently or temporarily) providing the Services (or any features within the Services) to you or to users generally and may not be able to provide you with prior notice. We also retain the right to create limits on use and storage at our sole discretion at any time without prior notice to you.

The Services may include advertisements, which may be targeted to the Content or information on the Services, queries made through the Services, or other information. The types and extent of advertising by Twitter on the Services are subject to change. In consideration for Twitter granting you access to and use of the Services, you agree that Twitter and its third party providers and partners may place such advertising on the Services or in connection with the display of Content or information from the Services whether submitted by you or others.

Privacy

Any information that you provide to Twitter is subject to our Privacy Policy, which governs our collection and use of your information. You understand that through your use of the Services you consent to the collection and use (as set forth in the Privacy Policy) of this information, including the transfer of this information to the United States and/or other countries for storage, processing and use by Twitter. As part of providing you the Services, we may need to provide you with certain communications, such as service announcements and administrative messages. These communications are considered part of the Services and your Twitter account, which you may not be able to opt-out from receiving.

Passwords

You are responsible for safeguarding the password that you use to access the Services and for any activities or actions under your password. We encourage you to use “strong” passwords (passwords that use a combination of upper and lower case letters, numbers and symbols) with your account. Twitter cannot and will not be liable for any loss or damage arising from your failure to comply with the above requirements.
Content on the Services

All Content, whether publicly posted or privately transmitted, is the sole responsibility of the person who originated such Content. We may not monitor or control the Content posted via the Services and, we cannot take responsibility for such Content. Any use or reliance on any Content or materials posted via the Services or obtained by you through the Services is at your own risk.

We do not endorse, support, represent or guarantee the completeness, truthfulness, accuracy, or reliability of any Content or communications posted via the Services or endorse any opinions expressed via the Services. You understand that by using the Services, you may be exposed to Content that might be offensive, harmful, inaccurate or otherwise inappropriate, or in some cases, postings that have been mislabeled or are otherwise deceptive. Under no circumstances will Twitter be liable in any way for any Content, including, but not limited to, any errors or omissions in any Content, or any loss or damage of any kind incurred as a result of the use of any Content posted, emailed, transmitted or otherwise made available via the Services or broadcast elsewhere.

Your Rights

You retain your rights to any Content you submit, post or display on or through the Services. By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).

You agree that this license includes the right for Twitter to make such Content available to other companies, organizations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such Content on other media and services, subject to our terms and conditions for such Content use.

Such additional uses by Twitter, or other companies, organizations or individuals who partner with Twitter, may be made with no compensation paid to you with respect to the Content that you submit, post, transmit or otherwise make available through the Services.

We may modify or adapt your Content in order to transmit, display or distribute it over computer networks and in various media and/or make changes to your Content as are necessary to conform and adapt that Content to any requirements or limitations of any networks, devices, services or media.

You are responsible for your use of the Services, for any Content you provide, and for any consequences thereof, including the use of your Content by other users and our third party partners. You understand that your Content may be rebroadcasted by our partners and if you do not have the right to submit Content for such use, it may subject you to liability. Twitter will not be responsible or liable for any use of your Content by Twitter in accordance with these Terms. You represent and warrant that you have all the rights, power and authority necessary to grant the rights granted herein to any Content that you submit.

Twitter gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software that is provided to you by Twitter as part of the Services. This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Twitter, in the manner permitted by these Terms.

Twitter Rights

All right, title, and interest in and to the Services (excluding Content provided by users) are and will remain the exclusive property of Twitter and its licensors. The Services are protected by copyright, trademark, and other laws of both the United States and foreign countries. Nothing in the Terms gives you a right to use the Twitter name or any of the Twitter trademarks, logos, domain names, and other distinctive brand features. Any feedback, comments, or suggestions you may provide regarding Twitter, or the Services is entirely voluntary and we will be free to use such feedback, comments or suggestions as we see fit and without any obligation to you.

Restrictions on Content and Use of the Services

We reserve the right at all times (but will not have an obligation) to remove or refuse to distribute any Content on the Services and to terminate users or reclaim usernames. Please review the Twitter Rules (which are part of these Terms) to better understand what is prohibited on the Service. We also reserve the right to access, read, preserve, and disclose any information as we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process or governmental request, (ii) enforce the Terms, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of Twitter, its users and the public.

Except as permitted through the Services (or these Terms), you have to use the Twitter API if you want to reproduce, modify, create derivative works, distribute, sell, transfer, publicly display, publicly perform, transmit, or otherwise use the Content or Services.

You may not do any of the following while accessing or using the Services: (i) access, tamper with, or use non-public areas of the Services, Twitter’s computer systems, or the technical delivery systems of Twitter’s providers; (ii) probe, scan, or test the vulnerability of any system or network or breach or circumvent any security or authentication measures; (iii) access or search or attempt to access or search the Services by any means (automated or otherwise) other than through our currently available, published interfaces that are provided by Twitter (and only pursuant to those terms and conditions), unless you have been specifically allowed to do so in a separate agreement with Twitter (NOTE: crawling the Services is permissible if done in accordance with the provisions of the robots.txt file, however, scraping the Services...
without the prior consent of Twitter is expressly prohibited; (iv) forge any TCP/IP packet header or any part of the header information in any email or posting, or in any way use the Services to send altered, deceptive or false source-identifying information; or (v) interfere with, or disrupt, (or attempt to do so), the access of any user, host or network, including, without limitation, sending a virus, overloading, flooding, spamming, mail-bombing the Services, or by scripting the creation of Content in such a manner as to interfere with or create an undue burden on the Services.

Copyright Policy

Twitter respects the intellectual property rights of others and expects users of the Services to do the same. We will respond to notices of alleged copyright infringement that comply with applicable law and are properly provided to us. If you believe that your Content has been copied in a way that constitutes copyright infringement, please provide us with the following information: (i) a physical or electronic signature of the copyright owner or a person authorized to act on their behalf; (ii) identification of the copyrighted work claimed to have been infringed; (iii) identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit us to locate the material; (iv) your contact information, including your address, telephone number, and an email address; (v) a statement by you that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and (vi) a statement that the information in the notification is accurate, and, under penalty of perjury, that you are authorized to act on behalf of the copyright owner.

We reserve the right to remove Content alleged to be infringing without prior notice and at our sole discretion. In appropriate circumstances, Twitter will also terminate a user’s account if the user is determined to be a repeat infringer. Our designated copyright agent for notice of alleged copyright infringement appearing on the Services is:

Twitter, Inc.
Attn: Copyright Agent
795 Folsom Street, Suite 600
San Francisco, CA 94103
Email: copyright@twitter.com

The Services are Available “AS-IS”

Your access to and use of the Services or any Content is at your own risk. You understand and agree that the Services is provided to you on an “AS IS” and “AS AVAILABLE” basis. Without limiting the foregoing, TWITTER AND ITS PARTNERS DISCLAIM ANY WARRANTIES, EXPRESS OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. We make no warranty and disclaim all responsibility and liability for the completeness, accuracy, availability, timeliness, security or reliability of the Services or any content thereon. Twitter will not be responsible or liable for any harm to your computer system, loss of data, or other harm that results from your access to or use of the Services, or any Content. You also agree that Twitter has no responsibility or liability for the deletion of, or the failure to store or to transmit, any Content and other communications maintained by the Services. We make no warranty that the Services will meet your requirements or be available on an uninterrupted, secure, or error-free basis. No advice or information, whether oral or written, obtained from Twitter or through the Services, will create any warranty not expressly made herein.

Links

The Services may contain links to third-party websites or resources. You acknowledge and agree that we are not responsible or liable for: (i) the availability or accuracy of such websites or resources; or (ii) the content, products, or services on or available from such websites or resources. Links to such websites or resources do not imply any endorsement by Twitter of such websites or resources or the content, products, or services available from such websites or resources. You acknowledge sole responsibility for and assume all risk arising from your use of any such websites or resources.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TWITTER AND ITS SUBSIDIARIES, AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF PROFITS, DATA, USE, GOOD-WILL, OR OTHER INTANGIBLE LOSSES, RESULTING FROM (i) YOUR ACCESS TO OR USE OF OR INABILITY TO ACCESS OR USE THE SERVICES; (ii) ANY CONDUCT OR CONTENT OF ANY THIRD PARTY ON THE SERVICES, INCLUDING WITHOUT LIMITATION, ANY DEFAMATORY, OFFENSIVE OR ILLEGAL CONDUCT OF OTHER USERS OR THIRD PARTIES; (iii) ANY CONTENT OBTAINED FROM THE SERVICES; AND (iv) UNAUTHORIZED ACCESS, USE OR ALTERATION OF YOUR TRANSMISSIONS OR CONTENT, WHETHER BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE) OR ANY OTHER LEGAL THEORY. WHETHER OR NOT TWITTER HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGE, AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

Exclusions

Some jurisdictions do not allow the exclusion of certain warranties or the exclusion or limitation of liability for consequential or incidental damages, so the limitations above may not apply to you.
Waiver and Severability

The failure of Twitter to enforce any right or provision of these Terms will not be deemed a waiver of such right or provision. In the event that any provision of these Terms is held to be invalid or unenforceable, the remaining provisions of these Terms will remain in full force and effect.

Controlling Law and Jurisdiction

These Terms and any action related thereto will be governed by the laws of the State of California without regard to or application of its conflict of law provisions or your state or country of residence. All claims, legal proceedings or litigation arising in connection with the Services will be brought solely in San Francisco County, California, and you consent to the jurisdiction of and venue in such courts and waive any objection as to inconvenient forum. If you are accepting these Terms on behalf of a United States federal government entity that is legally unable to accept the controlling law, jurisdiction or venue clauses above, then those clauses do not apply to you but instead these Terms and any action related thereto will be will be governed by the laws of the United States of America (without reference to conflict of laws) and, in the absence of federal law and to the extent permitted under federal law, the laws of the State of California (excluding choice of law).

Entire Agreement

These Terms, the Twitter Rules and our Privacy Policy are the entire and exclusive agreement between Twitter and you regarding the Services (excluding any services for which you have a separate agreement with Twitter that is explicitly in addition or in place of these Terms), and these Terms supersede and replace any prior agreements between Twitter and you regarding the Services.

We may revise these Terms from time to time, the most current version will always be at twitter.com/tos. If the revision, in our sole discretion, is material we will notify you via an @Twitter update or e-mail to the email associated with your account. By continuing to access or use the Services after those revisions become effective, you agree to be bound by the revised Terms.

These Services are operated and provided by Twitter Inc., 795 Folsom Street, Suite 600, San Francisco, CA 94103. If you have any questions about these Terms, please contact us.

Effective: September 18, 2009