ISSUE 14, NOVEMBER 2011

THE UNIVERSITY of ADELAIDE

# Unilink

## Legal & Risk Newsletter

## In this issue. . .



## Airline fined after breaching the Spam Act

Virgin Blue was recently given a hefty fine by the Australian Communications and Media Authority for breaching the Spam Act 2003 (Cth), when numerous Virgin Blue customers complained that they were unable to unsubscribe from the airline's mailing list.

Technical problems with Virgin Blue's email marketing system were blamed for the breach, which cost the airline $110,000 and has led to an overhaul of its email marketing practices, employee training program and complaints handling policy.

The company also agreed to conduct monthly audits of 10 percent of its email marketing campaigns for a year, to monitor its compliance with the Spam Act.

The presiding judge in the case said that while the incidents occurred mid last year, and while Virgin stopped sending messages as soon as they knew technical issues had occurred, "the company should have reasonably known something was happening".

Last March, the airline's sister company Virgin Mobile was also fined $22,000 for sending messages to customers who had 'opted out' of its mailing lists.


### Take-home message:

If you work in an area of the University that regularly uses email to communicate with potential students or alumni, ensure that the unsubscribe function in your email messages is working properly.

*For more information about your obligations under the Spam Act 2003 (Cth), see the Spam Act 101 available on the Resources page of the Legal & Risk website*

## IT Acceptable Use & Security Policy

The University's IT Acceptable Use and Security Policy and its associated procedures have recently been revised. The revised Policy includes;

- A new definition of 'IT facilities and services' to include social media and mobile communication devices,
- An addition to explicitly cover third party providers; and
- A flexibility to allow for additional logging, monitoring and blocking of web traffic.

While a more detailed article dealing with the issues surrounding social media will be included in a future newsletter, it should be remembered that when using social media, the standard laws, policies, professional expectations and guidelines for interacting within and outside the University community apply. The University is required to follow the same behavioural standards online, as it does in spoken and print communications.

### Key obligations of people using the University's IT facilities:

- Remember that **ALL** use of IT facilities and services is logged and monitored.
- Do not access pornographic or obscene material or material that could reasonably offend others.
- Think carefully about your online conduct to protect personal information.
- Do not use IT facilities to bully or harass others.
- Keep your password and account information private. Do not share it with anyone.
- Do not use IT facilities to advertise goods or services (aside from "University" goods and services).
- Only download videos, music and other content lawfully and in accordance with the University's statutory licences (refer Copyright website).
- Do not install unlicensed or malicious software.
- Consider your online behaviour and printing habits. Remember that every website you visit or page that you print costs the University money.

Refer to the ITS website for the complete list of Do's and Don'ts.

*For more information contact Melissa Gibbs (Senior Administration & Policy Officer, Infrastructure, Property & Tech) on 8313 8357 or email melissa.gibbs@adelaide.edu.au.*

### From the General Counsel

Welcome to an IT-focused edition of Unilink—linking you with legal, risk, compliance, contract and insurance issues.

The rise of social media and mobile networks has presented new opportunities for engagement and also new risks to be managed. In this edition we delve deeper into how reputational risk can undermine the public's perception of Universities, and discuss why having clear internet and social media guidelines is so important (pg4).

The recently revised IT Acceptable Use and Security Policy which governs our use IT and goes some way towards protecting the University from reputational risk. We introduce this new policy and outline some of its key points.

Many thanks to Veronica Scott (Minter Ellison) and Melissa Gibbs (Infrastructure, Property & Technology) who contributed the two IT articles.

We are now over half way through our roll-out of the Legal Compliance Framework, and thought it pertinent to reflect on what we've learned, what areas are scheduled next and how you could be involved. Turn to page 2 for our double-page spread.

As this is the final issue of 2011, on behalf of the Legal & Risk team, I would like to thank you for your engagement with us during 2011 and wish all of you a safe and enjoyable Christmas.

Celine McInerney, General Counsel

Unilink

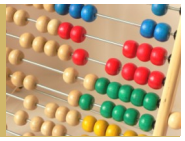
Legal & Risk Newsletter

## For more information

More detailed information about the legal compliance framework, the roll-out, the people involved, and the resources available to assist you, is available on the legal compliance website: www.adelaide.edu.au/legalandrisk/compliance/

# Legal Compliance—by the numbers

As you would know from earlier editions of Unilink, Legal & Risk is rolling out a legal compliance framework across the University. This has involved many presentations explaining the framework: its importance, how it works and what you need to do about it. Rather than explaining it again here as part of our 2011 wrap up, we thought it would be interesting to look at the numbers behind the words – after all, who doesn't love statistics?



**215** Acts (both State and Federal) apply to the University and its controlled entities. A list of these Acts is available on the legal compliance website.

**5** The Acts are classified across five tiers to prioritise them from the most significant, to those that have negligible consequence.

**3159** University staff that are all impacted by the legislation, not to mention contractors, titleholders and volunteers.

**1** Legal Compliance Policy formally affirming the University's commitment to compliance and establishing a framework to assist staff meet their compliance obligations.

**½** We are just over half-way through rolling out the framework (scheduled for 2010 to 2012).

**30** Areas have adopted the framework so far, covering all five faculties, the divisions and controlled entities.

**150** Meetings and presentations held since the rollout began, ranging from high level briefings, to in-depth discussions and tailored training on particular Acts.

**240** University staff now trained in the framework.

**3** Steps required for an area to adopt the framework:
1) a one hour discussion to identify the legislation that applies
2) a one hour training session, and
3) a 15 minute presentation to all staff.

**4** The legal compliance framework is a four step process:
1) identify legislation and assign responsibility
2) disseminate the requirements (communicate and educate)
3) monitor compliance (and assist if something goes wrong)
4) certify (confirm compliance on an annual basis)

**18** Categories of legislation that apply to all (or most) areas of the University, (e.g. Intellectual Property or Research Ethics). The legislation in these categories is listed on the legal compliance website.

**8** University Compliance Owners responsible for compliance by the University with those categories of legislation, e.g. DVC&VP (R) or General Counsel. UCOs assist schools or areas to meet their legal obligations through policies, processes, systems, training and any other necessary support mechanisms.

**36** Designated Specialist Officers, who are subject matter experts for the legislation that applies across the University.

DSOs are available to assist schools or areas with any legislative queries or concerns. They have been identified for each Act that applies across the University and their contact details are available on the legal compliance website.

**36** Acts that apply specifically (and sometimes only) to a particular school or area, e.g. the Veterinary Practice Act applies to the School of Animal & Veterinary Sciences.

The school or area is responsible for compliance with these Acts, as well as the numerous other Acts that apply more generically across the University, e.g. the Equal Opportunity Act, the Competition and Consumer Act or the Spam Act.

**33** Local Area Heads responsible for compliance with all legislation that applies to their school or area. This number will increase as the roll-out continues.

Local Area Head is a generic term for Head of School, Director of Branch or General Manager of a controlled entity – the head of any area. They are responsible for compliance by their area with all applicable legislation. For those Acts that apply across the University, this is achieved by adopting the relevant policies, processes and systems. For Acts specific to the school or area, compliance is managed locally.

The legislation that applies to each school or area is listed on the legal compliance website.

**150** Local Compliance Officers assisting Local Area Heads manage compliance on a day-to-day basis. This number will increase as the roll-out continues

LCOs are staff who have a general understanding of the school or area and its compliance activities (e.g. School Manager) or detailed knowledge of a particular Act that applies to the area (e.g. technical specialist). They are the first point of contact for compliance matters within an area.

The LCOs for each school or area are shown on the legal compliance website.

**25** Summaries of key Acts available on the Legal & Risk website, plus links to existing compliance material already on the University website or on external sites.

**102** Legal alerts issued to staff advising of changes to legislation affecting the University.

These include recent changes to Trade Licensing, Occupational Health & Safety, Trade Practices, Business Names, Privacy, TEQSA (Tertiary Education Quality Standards Agency), ESOS (Education Services for Overseas Students), Health Practitioner Registration and Personal Properties Securities.

**33** Compliance matters reported through the framework.

Compliance matters are instance of non-compliance or potential non-compliance. They are called compliance matters to re-enforce the positive aspects of compliance and to protect the University's position and that of any staff member.

**27** Compliance matters resolved.

# Unilink

**Legal & Risk Newsletter**

## Remember. . .

Legal Compliance is everyone's responsibility at some level, and every day. Individual commitment to a compliance culture is a critical factor in achieving compliance on a University-wide scale.

# Legal Compliance—by the numbers

**14** Editions of Unilink newsletter published since 2009– promoting an awareness of legal, contract, risk, compliance and insurance issues.

**121,000** The potential fine to the University for an inadvertent breach of the Commonwealth Electoral Act. As the University responded quickly following the breach, a formal reprimand was issued, but the fine was waived.

**1** Legal compliance certification.

Each year, senior managers provide a certificate of compliance to the Vice-Chancellor. These are collated to create a compliance certification for the University as a whole. The first certification was completed for 2010 and, in conjunction with adopting the framework, has allowed the University to demonstrate compliance both internally and to its regulators.

**17** Areas scheduled to adopt the framework in 2012.

**#34539** The number to call if you have any questions.

## The Legal Compliance Team

**G07 Mitchell Building**

Celine McInerney, General Counsel
celine.mcinerney@adelaide.edu.au
(08) 8313 0482

Richard Boyer, Manager Compliance
richard.boyer@adelaide.edu.au
(08) 8313 0482

Phillipa Schliebs, Project Officer
phillipa.schliebs@adelaide.edu.au
(08) 8313 4539

**Thank you to all the areas that have adopted the framework. We look forward to working with you and other areas of the University through 2012 and beyond.**

# Commonwealth v. State Law

We were asked as part of the compliance program recently, *"why do we have Commonwealth as well as State law?"* Here's the simple answer...

Australia was originally a collection of separate colonies and each colony made laws that operated within their "jurisdiction". With federation in 1901, the "Commonwealth of Australia" was established and the six colonies were united under a national government. This is known as a "federal system". The Australian Constitution established the parliament of the Commonwealth of Australia and acknowledged the continued existence of the colonies as states of the Commonwealth.

Some powers are exclusive to the Commonwealth (e.g. customs and excise, the currency, defence forces). Most Commonwealth powers are concurrent, meaning that both the Commonwealth and the State can enact legislation (e.g. trading / financial corporations, banking, quarantine). However the Constitution provides that where a state law is inconsistent with a law of the Commonwealth, the federal law will prevail. State governments retain residual powers to regulate matters not within the Constitution (e.g. education, transport, local government).

### But there seem to be national laws on matters not set out in the Constitution…

For some Commonwealth legislation, the Constitutional basis may not be immediately apparent. For example, the various Commonwealth anti-discrimination Acts were enacted on the basis of the Commonwealth's 'external affairs' power. As a signatory to international treaties, the Commonwealth needed to enact legislation to give effect to those treaties. The Commonwealth has also relied on its power in relation to "trading and financial corporations" to legislate on a wide range of activities and behaviours of such corporations, e.g. trade practices, consumer protection, privacy, industrial relations. Additionally, the Constitution enables States to refer their powers to the Commonwealth.


This has happened for terrorist acts (2002) and industrial relations for private sector businesses (2009). However States are more likely to choose to enact their own State legislation that adopts a uniform national regime, rather than refer their powers to the Commonwealth. Examples of these in South Australia are the *Defamation Act 2005*; *Health Practitioner Regulation National Law (South Australia) 2010;* and amendment of the *Fair Trading Act* in 2010 to adopt the Australian Consumer Law. The State Parliament is currently debating the adoption of uniform OHS legislation. In the future, it is also expected that uniform Privacy laws will be adopted across the country.

### What happens if there is both Commonwealth and State law on the same subject matter?

If two sets of laws apply, we must comply with both. For example, if you are seeking to import plants, you will have to comply with requirements under the *Quarantine Act (Cth)* for bringing the plants into Australia, and you will also have to comply with the *Plant Health Act (SA)* if you wish to bring the same plants into South Australia.

In some cases, such as anti-discrimination legislation, Federal and State laws may actually overlap. Compliance requirements will not differ, as State legislation will be invalid if it is inconsistent with the Commonwealth's. What it does mean is that a complainant may have the option of bringing an action under the State or Commonwealth jurisdiction, but not both. For example, a person may choose to lodge a complaint with the Australian Human Rights Commission under the relevant Commonwealth anti-discrimination legislation, or with the South Australian Equal Opportunity Commission under the *Equal Opportunity Act (SA)*. The outcomes available may differ too.

*For more information, contact Geraldine Yam (Legal Counsel) on 8313 5244 or email geraldine.yam@adelaide.edu.au.*

# Unilink

**Legal & Risk Newsletter**

**Top Risk Concerns—2010/11**

The latest AON Australiasian Risk Management Benchmarking Survey showed that for the fourth year running, "Brand and Image" ranked as the number one risk concern amongst businesses. "Increased use of social networks" was specifically cited as providing potential risk to an organisation's brand, image and reputation.

# Universities - reputational risk from the internet

**Reputation is critical to a university's success. Attacks on reputation can come from a range of sources. The rise of social media and mobile networks can expose universities to serious reputational risk and undermine the public's perception of them as places of serious research and education.**

According to the *Student Grievances and Discipline Matters Project* Final Report to the Australian Learning and Teaching Council, the overwhelming majority of legal or quasi-legal complaints against universities have been successfully defended. However, a legal win is not necessarily a good news story for the university. Reputation can be a casualty as a result of disengaged students and staff using social media such as blogs and gripe sites to voice their complaints and disseminate negative content. Publicity is their weapon, harming not only the reputation of the university, but the privacy and reputations of its students and staff, especially if content goes viral. Data is also preserved in cyberspace forever and can be easily revitalised even after the story dies down.


The new Unileaks site is one of the most recent examples of an online forum for anonymous disclosures and whistleblowers. The site describes itself as a news organisation that will 'accept restricted or censored material...'. The ability to post anonymous content means people may take risks, as they cannot easily be identified and the ISP or website operator stands in front of them as the main target of complaints and actions.

The legal options for universities facing the publication of false and damaging statements are quite limited. Corporations and public bodies, which include universities, are now generally prohibited from suing for defamation (see section 9 of the uniform *Defamation Acts*). An individual associated with the university can sue personally for defamation if they are also identified and harmed by the same statements.

A university could sue for misleading and deceptive conduct under the provisions in section 52 of the *Trade Practices Act 1974* (**TPA**), which are now found in section 18 of the *Australian Consumer Law* (**ACL**) at Schedule 2 to the *Competition and Consumer Act 2010* (the new name for the TPA). These provisions capture the acts of individuals as well as corporations who, in trade or commerce, engage in misleading and deceptive conduct. 'Trade or commerce' includes any business or professional activity, whether or not carried out for profit. Therefore, bloggers, ISPs, and operators of online forums and bulletin boards can be caught.

While many individuals (eg students) are unlikely to be publishing comments online or to the media in the course of trade or commerce, academic staff who publish online in their professional capacity could fall within the scope of the section. However, section 18 has limited application to media and news organisations because section 19 of the ACL (previously section 65A of the TPA) protects them if they publish the statements in the course of carrying on their business of providing information. Universities should therefore also take care that their academic staff do not expose themselves, and potentially the university, to claims under section 18, as they do not have the same protection as the media under section 19.

MinterEllison LAWYERS

Almost everyone is sharing information online, chatting and gossiping about their lives and about other people. However, private information, opinions and rumours can quickly go viral. A picture taken or an act filmed on a mobile phone by a student on campus can be uploaded to Facebook or Youtube, then mashed up, blogged, twittered about, and even taken up by the mainstream media. It can turn into cyberbullying and harassment, with serious consequences for individuals as well as the university. This could involve the university taking disciplinary action against a student for misconduct, as well as the commission of a criminal offence - for example, under the Victorian *Surveillance Devices Act 1999*, which prohibits a person from recording a private activity or conversation they are not part of without consent and publishing it or the Commonwealth *Criminal Code 1995*, which makes it an offence to use a carriage service in a way that reasonable people would regard as being, in all the circumstances, menacing, harassing or offensive.

Universities need to manage the risks to their reputation from the internet in the same way they manage other aspects of university life, such as human resources, intellectual property and student complaints and grievances. This starts with clear internet and social media guidelines for students and staff and actively fostering the responsible use of social networks, mobile devices and the internet generally. Legal redress for reputational damage may be available in certain circumstances, but is limited and can be slow to achieve results.

*This article was written by Veronica Scott, Senior Associate, Minter Ellison law firm. For more legal articles about higher education, refer to Minter Ellison's online publication - Higher Education Focus.*

# New Compliance Resources

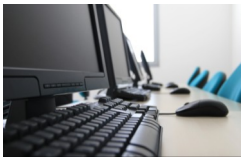
Many useful internal and external publications and weblinks can be found on the Resources page of the Legal & Risk website. New summaries of key Acts include:

- Aboriginal Heritage Act 1988 (SA)
- Native Title Act 1993 (Cth)
- Health Practitioner Regulation National Law (South Australia) Act 2010 (SA)

These summaries provide an overview of an Act as it applies specifically to the University. The short power-point presentations are set out in easy-to-read language, explain the Act in the context of the University, outline the main obligations of staff, and provide reference points for further information or advice.

# New IT Resources

The IT Best Practice Guidelines have recently been reviewed and several new sets have been added, including:



- Calendar Best Practice
- Use of Library e-Resources
- Posting on MyUni Forums
- Social Media.

For these resources and many more, go to the IT Policies, Procedures and Best Practice Guidelines webpage on the Infrastructure, Property and Technology website.