University and College Union

Health and safety factsheet

Practical steps to ensure internet safety

If you're using the internet, you should **never give out your personal details**. If you're in a chatroom, watch what you say about where you live, where you work, or your email address.

As well as allowing a cyber-bully to build up a picture about you and how they can hurt you, posting personal information online can attract the perpetrator who often lies about their real identity.

Social networking sites

Social networks are a great way of keeping in touch but you should think carefully before adding someone to your list of online friends or posting a blog entry that could get you into trouble at work. Remember that:

- **Your page is still a public place, so putting anything on your page that you wouldn't want others to see is not a good idea**
- **You can never be sure that other users are being truthful about their online identities, so be careful about what information you give out**
- **Think about whether you know someone well enough before accepting someone into your group of linked friends**
- **Make sure you know who to contact to report abuse or bullying on your page and how your complaint will be dealt with**

Chat room safety

To stay safe, make sure that when you're using a chat room or posting on a message board, you never give out any personal information like your address or your phone number. You should always use a nickname, so no-one can look you up in a telephone directory and get your home phone number.

Personal details

Some websites will ask you to fill out a registration form before you can use them. While this is normal practice, it's a good idea to find out what the website will do with your personal details. All companies that collect information have to tell their customers how personal information will be used. Make sure you check the website's terms and conditions if you want to know.

Some sites allow other companies to use details from their user database for market research purposes. Companies have to give you the chance to tell them if you don't want your details to be used in this way.

This is often done by having a tick box on the online registration page. If you don't want your information to be used for marketing purposes, make sure you tick that box before you submit your information.

Many people are still reluctant to shop on the internet because they believe that their bank details are not safe. Luckily, shopping on the web is now just as safe as ordering goods over the telephone, as long as you follow a few common sense rules.

Make sure that if you do order goods over the Internet, the company that you're buying from uses a secure shopping server. You'll know if it is a secure site if a padlock icon 🔒 appears at the bottom of your browser window, or the web address begins with 'https:'

If it's a company that you've never heard of before, search their site for any contact numbers and postal addresses. If they're a respectable company, they won't mind if you give them a quick call to ask them a few questions.

Also, make sure that you never send your bank details to anyone in an email. Legitimate banks and online stores will never ask you to do this as it is not a secure way of sending information.

If you do receive an official-looking email that asks you to send your financial details, you should never reply as you could become a victim of identity fraud.

Can the perpetrator be traced?

No matter how careful the offender is to cover their tracks, there is no hiding in cyberspace; the police can track digital fingerprints down to an individual computer or mobile phone.

Organisations such as **BullyingUK** can actually take steps to close down abusive websites and internet forums and in the past they have also passed on details of any abuse to the police.

For example: If you are named on an internet chat room or forum in a manner which constitutes bullying, reporting this to the website can actually get the people naming you removed as users. Even if they are using false names, the company that hosts the website can still track down their computer.

A police officer will be able to enforce the law around cyber-bullying to ensure that something can be done about it. Contacting the service provider, such as the mobile operator or the Instant messenger or social network provider to report what has happened can also be a useful step.

What are the laws around cyber-bullying?

The law provides a number of possible remedies for people suffering from cyber-bullying or other forms of Harassment. You should **NOT** try to institute legal proceedings of any kind without taking advice from UCU. The summary of the legal position which follows is for information only and is not intended as a guide to taking action yourself.

However your first step should be to get your employer to enforce their policies and take action where the perpetrator is known. This should be done through UCU locally. The outcome of prosecutions is always uncertain and your immediate priority should be to approach your employer, after taking UCU advice, and seek to get the employer to exercise its duty of care towards its staff and protect them from cyber-bullying.

For further information, see our factsheet on Cyber-bullying.

The law

Under **Section 1 of the Malicious Communications Act 1998** it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person and under **Section 43 of the Telecommunications Act 1984** it is a similar offence to send a telephone message which is indecent offensive or threatening. In both cases the offence is punishable with up to six months imprisonment and/or a fine of up to £5000.

Because the **Malicious Communications Offence** is wider ranging than the Telecommunications offence it is more likely to be used by the Police than the Telecommunications Act offence.

In most cases involving malicious communications or cyber-bullying however there will be more than one offensive or threatening letter or telephone call and therefore the police will often choose to charge the offender with an offence contrary to either **Section 2 of the Protection from Harassment Act 1997** also punishable with up to six months imprisonment.

Part of the reason for using this charge is that when someone is convicted of an offence under the **Protection from Harassment Act 1997** the court can make a Restraining Order preventing them from contacting their victim again.

Breach of a Restraining Order is punishable with up to Five years imprisonment. A Restraining Order cannot be imposed for a conviction under the Malicious Communications or Telecommunications Acts.

If the e-mails, cyber-bullying etc. causes the victim to fear that violence will be used against them then the police can choose to charge the offender with an offence contrary to **Section 4 of the Protection from Harassment Act 1997** which is punishable with up to five years imprisonment and also allows the court to make a Restraining Order.

If the e-mails, cyber-bullying etc. is racialist in nature or motivated by religious hostility then charges could be brought of **Racially or Religiously Aggravated Harassment** contrary to sections 32(1)(a) or 32(1)(b) of the Crime and Disorder Act 1998 . If convicted offenders could face up to 7 years imprisonment.

The fact that an offensive telephone call, letter e-mail etc. may be received in the course of work and have been sent by a work colleague or manager does not justify the message or prevent it being an offence. Offensive messages sent within the workplace can still constitute criminal offences. In addition they may justify a claim for constructive dismissal and compensation under employment law.

In many situations the recipient of malicious messages knows who the sender is. It may be a former partner or a relative which may mean that the victim is reluctant to involve the police. In those circumstances the victim could consider taking out an Injunction under **Section 3 of the Protection from Harassment Act 1997**. However we would always advise informing the police especially if the messages are in any way threatening. Even if the police decide not to prosecute they may give the offender a formal warning which could be used in evidence if they repeated their behaviour in future.

In addition to criminal prosecutions victims of harassment can sue the offender under **Section 3 of the Protection from Harassment Act 1997** for damages arising out of the anxiety caused by the Harassment and any financial loss it caused.

What if the offender is outside of the UK?

Where the offender has sent the message from outside England and Wales the Police will usually inform their foreign counterparts.
It will frequently be the case that the offender has also broken the law in his own jurisdiction and will be dealt with by the authorities in that jurisdiction.

Similarly if someone in England and Wales is harassing someone abroad by means of letters e-mails etc. and the Police in England and Wales are informed of this then the offender could be arrested for criminal harassment and prosecuted regardless of the fact the victim was abroad.

Resources and further information

Bullying and harassment are a major hazard for UCU members. If you are affected by bullying (in whatever form) or want to do something about it you may find the following materials useful:

University and College Union	Stop bullying and harassment at work - A handbook for UCU reps and members on essential steps to take to prevent bullying and harassment – and supporting members affected by it. **www.ucu.org.uk/index.cfm?articleid=3314** Factsheet on Cyber-bullying **http://www.ucu.org.uk/hsfacts - being online**
College and University Support Network (CUSN)	The College and University Support Network (CUSN) offers free 24hr support services to all staff in further and higher education and their families, including confidential counselling, solution-focused counselling on personal and workplace issues. **www.cusn.info or telephone 08000 32 99 52**
Association of Colleges	UCU and other unions have reached a national agreement with the Association of College for all FE colleges which branches and LAs can use as a model for local implementation covering bullying and harassment, including Cyber-bullying. **www.ucu.org.uk/media/docs/4/l/feagrhar.doc**
Health and Safety Executive	Management Standards for Work Related Stress, Tackling Work related stress in education and Guidance for Safety Representatives **www.hse.gov.uk**
Teachernet	Resources for teachers **publications.teachernet.gov.uk/eOrderingDownload/Cyber bullying-leaflet.pdf**
ACAS	Guidance on bullying and harassment **www.acas.org.uk**
Labour Research Department	Tackling bullying and harassment - a trade unionist's guide **www.lrd.org.uk**
Trades Union Congress	See TUC health and safety pages **www.tuc.org.uk**
The Andrea Adams Trust	Leading anti-bullying charity **www.andreaadamstrust.org**