**What is social media bullying?**

Social media has brought with it bullying in a new form - through the internet.
Bullying through technology is not always so tangible - the victim may not see it, though their colleagues may, and it can carry on online away from the workplace.

**Social networking**

**The risks**

* disclosure of private information by either yourself or friends/contacts
* bullying
* cyber-stalking
* prosecution or recrimination from posting offensive or inappropriate comments
* people hacking into or hijacking your account or page
* viruses or spyware contained within message attachments or photographs
* you or a family member posting that you're away or going away on holiday and therefore advertising that your home is empty, leaving the way open for burglars. If you do so and you make an insurance claim for a burglary while you are away, your insurance company may well reject it for this reason.

**Safe social networking**

You can avoid these risks and enjoy using social networking sites by following a few sensible guidelines:

* Be wary of publishing any identifying information about yourself – either in your profile or in your posts – such as phone numbers, pictures of your home, workplace, your address or birthday.
* Pick a user name that does not include any personal information. For example, “joe\_glasgow” or “jane\_liverpool” would be bad choices.
* Set up a separate email account to register and receive mail from the site, that way if you want to close down your account/page, you can simply stop using that mail account. Setting up a new email account is very simple and quick to do using such providers as Hotmail, Yahoo! Mail or gmail.
* Use strong passwords.
* Keep your profile closed and allow only your friends to view your profile.
* What goes online stays online. Do not say anything or publish pictures that might later cause you or someone else embarrassment.
* Never post comments that are abusive or may cause offence to either individuals or groups of society.
* Be aware of what friends post about you, or reply to your posts, particularly about your personal details and activities.
* Remember that many companies routinely view current or prospective employees’ social networking pages, so be careful about what you say, what pictures you post and your profile.
* Learn how to use the site properly. Use the privacy features to restrict strangers’ access to your profile. Be guarded about who you let join your network.
* Be on your guard against phishing, scams, including fake friend requests and posts from individuals or companies inviting you to visit other pages or sites.
* If you do get caught up in a scam, make sure you remove any corresponding likes and app permissions from your account.
* Ensure you have effective and updated antivirus/antispyware software software and firewall running before you go online.

For more information on security visit the social networking sites’ own online safety pages:

[Facebook](http://facebook.com/help/safety), [Twitter](http://support.twitter.com/articles/76036-safety-keeping-your-account-secure), [Bebo](http://bebo.com/Safety.jsp), [Myspace](http://uk.myspace.com/help/safety/tips), [YouTube](http://support.google.com/youtube/bin/request.py?&contact_type=abuse) and [Instagram](http://help.instagram.com/).

**Cyber bullying**

This is bullying, harassment and victimisation conducted through social media such as blogs or social networking sites. Inappropriate photographs, offensive or threatening comments or sensitive personal information might be posted vindictively. A manager or an employee might be targeted in the workplace which can manifest itself in many different forms. Nobody is immune to cyber bullying, but there are steps you can take and support available if you feel you have become a victim of cyber bullying at work.

Social media tools, such as smart phones and social networking sites, can be used so that bullying between staff can more easily be conducted out of working hours and away from work premises.

The victim may, or may not, be aware that they are being bullied. For example, while they are likely to see a threat emailed to them, they may not see comments on a social networking site.

**Risk of exclusion**

Managers and employees can sometimes feel pressure to join someone's online circle of 'friends' or work contacts. An employee might prefer not to accept an invitation, they might worry that to decline or ignore it could offend the sender, and cause a problem further down the line. Some staff can be uncomfortable either accepting or declining an invitation from their line manager or other senior members of the organisation.

**Examples of bullying at work using electronic means**

1. **Offensive e-mail**

Sending an offensive e-mail to a colleague (even if it's supposed to be a joke,) the content of which might offend the receiver. This includes any offensive photographs which are attached to an email, and continuing to send similar messages having been asked to stop.

1. **E-mail threats**

This can include relatively inoffensive messages in terms of content, but the implied meaning behind the message can constitute a form of bullying. An example of this might be where a senior workers, colleagues or manager is bombarding you with far more work than you can handle, saying that this is part of your job (i.e. If you don't complete the work you may lose your job) whilst other members of the team are not being treated in the same way.

1. **Posting blogs and comments on social networking sites**

Often a person may not experience any direct form of cyber bullying, but instead the bullies are leaving nasty or offensive comments about them on blogs and social networking sites which can be viewed by others. The comments may be about the person's performance at work, or more commonly can be personal.

1. **Spreading lies and malicious gossip**

Social networking sites and blogs are usually the most common ways in which people become victims of cyber bullying in this form.

Cyber bullying can occur via any electronic means including text messages, phone calls and social media (such as Facebook and Twitter).

**Intentional or Not?**

Cyber bullying harassment - electronic cyber bullying, or 'e-bullying' as it is often referred to, can also occur when the person may not even intend to harm you. This type of bullying is particularly concerning, as the bully is unlikely to stop their behaviour on their own, as they do not know that they are doing anything wrong.

The two main types of non-intentional cyber-bullying are:

**1. Persistence of an admirer**

You may experience an admirer at work who would like to establish a closer friendship or relationship with you. Admirers will sometimes use e-mail or social media to 'test the waters' first as the fear of rejection is often lessened if an approach is made that way. However, people have been rightfully prosecuted for sexual harassment where persistent electronic communication (texts/emails etc.) follows, especially if they have been rejected and told to stop. This type of cyber-bullying has even led to cases of stalking outside work and so is particularly important to prevent at an early stage.

**2. Invasion of privacy**

This type of bullying involves sharing someone's private data online. This can be posting any personal details which can be viewed by the general public, or other colleagues at work, which you would not normally want to share. Clearly giving your phone number privately to one other colleague on your team will not fall under the umbrella term bullying, but for example posting your personal telephone number or home address on a site which can be viewed by all your colleagues across the whole business (including other national offices) will do.

**How to deal with cyber bullying at work**

External cyber bullies who are operating outside your workplace, if they are emailing your work email, your work IT department should be able to stop this activity and can also take steps to identify the perpetrators. Remember - if you are being bullied, do not suffer in silence. Tell someone who will be able to help you stand up to the bullies. Nobody should make you feel uncomfortable at your place of work.

Whether it's e-bullying or face-to-face, there are laws surrounding both harassment and bullying in the UK, and you can take legal action if you feel you have become the victim of a cyber bully.

**Speak to the person**

Firstly, you should try to resolve the problem with the person directly if you know their identity. In some cases, it might be true that what you thought was offensive was not perceived as such by the sender and there has been some misunderstanding. In the case of invasion of privacy, it is often quite easy to 'nip this in the bud', and often your cyber bully will be extremely apologetic, not realising the problem they created, or how they made you feel.

**Speak to a manager**

If the bullying persists, you should go and speak to a manager (or Union Representative if you have one) to discuss the situation and to obtain support. Often they will be able to speak to the bully about their behaviour and tell them to stop. Fortunately, most companies will have strict policies on the use of e-mail and the internet at work and a person can lawfully be dismissed if the company policy is ignored or abused. The ICT Policy is available on KNET.

Inappropriate use of company email will often include:

* sending any personal emails (e.g. to ask someone on a date)
* to pass on "viral" videos or links to non-work related websites
* to mass email a joke (particularly one that is sexist, racist or homophobic).

**Consider a non-molestation order**

If the bullying still does not stop at the request of your manager, and the emails/text messages are regularly being sent despite you asking the other person to stop, this may be considered harassment. If so, you might be able to obtain a non-molestation order which makes it an offence for the offending party to contact you. Obviously a court cannot prevent you seeing a colleague at work, but they can order that the offending party does not contact you out of work via email, telephone, text message or social media.

Other simple ways to prevent a colleague contacting you out of work include:

1. blocking their number on your phone
2. blocking them on your social networking site.

Cyber bullying is no less unpleasant than conventional bullying. Always remember that you are protected by the law in just the same way as conventional bullying.

**What is stalking?**

Stalking can be defined as repeated, unwanted contact from one person to another which causes the victim to feel distressed or fearful. It differs from harassment in that a perpetrator will have an obsession with or fixation on the individual(s) they are targeting.

Stalking can take place in many forms in the workplace. Some stalkers are colleagues or clients of the victim, others are individuals who are unrelated to the workplace but who make contact with the victim there because of ease of access or to cause them further distress.

Stalking behaviour can include:

* nuisance telephone calls
* being followed
* death threats
* making false complaints to employers/police etc
* criminal damage
* blackmail
* sexual assault
* sending excessive emails
* sending gifts or letters
* monitoring behaviour
* abuse through social networking sites
* visiting home or place of work
* physical assault
* computer hacking.

**Stalking and the law**

Stalking is a specific criminal office in England under the Protection from Harassment Act 1997, amended by the Protection of Freedoms Act 2012.

**What can you do to help deal with possible stalking or harassment concerns?**

* If you are in immediate danger call 999.
* Report concerns to your line manager at the first signs of stalking or harassment and contact the Police non-emergency number 101.
* Consider your lone working safe systems of work to see what additional controls may need to implement.
* Collate as much evidence as possible to assist the police whether you have or have not reported the incident, e.g.
* keep a diary of events (date/time/location/details of what happened)
* keep copies of letters, text messages, emails and take screen shots of other online messages (e.g. social network platforms)
* try to get ‘evidence’ of any events that happen at your home but be careful to do this discreetly so as not to endanger yourself.
* Contact the National Stalking Helpline for advice and support on 0808 802 0300 [www.suzylamplugh.org/stalking](http://www.suzylamplugh.org/stalking)
* Contact Victim Support who can offer practical help and advice on 0808 1689111 [www.victimsupport.org.uk](http://www.victimsupport.org.uk)