



Professional boundaries in relation to your personal internet use and social networking online

Maintaining professional boundaries

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

Staff should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. Do not put yourself at risk by communicating with children outside of your organisation's boundaries. Communication with children you work with should always be via your organisation's networks.

Staff should not give their personal contact details to children and young people including email, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. If children contact you using your personal email or via social networking, do not respond but inform your line manager.

Understanding the risks

As well as the potential for young people you work with to contact you, you also need to be aware of accidentally bringing your workplace or your professional role into disrepute through inadvertently posting inappropriate comments about work on your profile, for instance, criticising policy or fellow colleagues. Remember, it's very difficult to control exactly who will end up seeing comments posted on social networking sites such as Facebook.

This guidance focuses mainly on the use of Facebook but the principles and advice are relevant to any social networking site.

How to protect your reputation and stay safe online

Act in accordance with your organisational policy.

E-mail or text communications between an adult and a child or young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Manage your personal information. Staff are strongly advised, in their own interests, to take steps to ensure their personal data is not accessible to anybody who does not have permission to access it. This includes your date of birth and address. Identity theft is a growing crime and this information could be used to access your bank account or apply for a credit card in your name.

Understand privacy. How you behave online is not the same as doing what you like in the privacy of your living room. As an employee you should be careful that your behaviour and conversations on the internet doesn't compromise your professional role. Privacy on the internet seldom means communications are entirely private, even messaging.

Respect dignity. Do not post pictures of or comments about children or young people you are working with. Respect people's right to confidentiality.

Uphold your reputation. Remember that anything posted online could end up in the public domain to be read by parents, children, young people or your employer. Some organisations may even access social networking sites before considering you for a job interview.

Further tips for Facebook and other social network sites

- Treat your online conversations as if you were talking with people in a public space where you can be seen and overheard
- Don't post or tweet when under the strong influence of alcohol or drugs
- Learn how to adjust your security or privacy settings in Facebook. Most social networking sites allow you to control who can see your information. For example, at the bottom of every page on Facebook, there is a link that reads 'Privacy'. The linked page is 'a guide to privacy on Facebook', containing the latest privacy functions and policies.
- Set your privacy settings to "only friends". Settings such as "friends of friends" and "networks and friends" open your content to a wider audience. Your privacy and that of your family, friends, colleagues and students could be compromised
- Remove inappropriate photos. Somebody else could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed.
- Make sure you regularly check and refresh your site page to ensure it is free of any inappropriate comments and/or images.
- Always log out of any conversations when you have finished using the site.
- Stop the network provider from passing on your details to other companies for research and advertising purposes.

How to report abuse

You should familiarise yourself with the information provided by Facebook on their Safety Help pages. You can find this here: <http://www.facebook.com/safety/>

Should you come across any potentially illegal, pornographic, offensive or otherwise inappropriate material, or conduct from a user of Facebook which you believe is illegal or offensive or unwelcome, you can use the 'Report' link located around the site. You can also email abuse@facebook.com with details.

Report an underage user	http://www.facebook.com/help/contact/?id=210036389087590
Account has been hacked	https://www.facebook.com/login/identify?ctx=login
False account created	http://www.facebook.com/help/contact/?id=169486816475808
Email account wrongly used	http://www.facebook.com/help/167722253287296/
Privacy issues with photos	https://www.facebook.com/help/contact/?id=473738729306832&rdrc
Cyberbullying information	http://www.facebook.com/help/420576171311103/
Hiding your profile from search engines	http://www.facebook.com/settings/?tab=privacy&section=applications&field=public_search&h=AQNL-D-G0iSB_asj4
Adjusting security settings	http://www.facebook.com/settings/?tab=privacy&ref=mb
Adjusting user settings	http://www.facebook.com/settings/?tab=privacy&ref=mb
Reporting if not a Facebook member	http://www.facebook.com/help/167722253287296/

Or use the Click CEOP report abuse button - <http://www.ceop.police.uk/>

The guiding rule is if in doubt, don't post it.