



New Technologies

- a personal health warning!

Guidelines for Student Teachers and NQTs



When using the internet

Think “How could it be abused?”

Any information, photos, videos and files on the internet can easily be made available to every internet user on the planet!! This includes friends, family, prospective employers and present colleagues and students and people you have not even met yet.

Photos, videos and information can be easily modified to cause further harm or embarrassment. Search engines find this information automatically. It is nearly impossible to remove – you have little support as there is no single legal protection.

Social networking sites such as YouTube, Facebook,

My Space can be used safely if you consider the information you are posting. Ensure that you use the privacy settings so that “only people you know” can see your site. If necessary, link your profile on other sites to your single main site, this keeps you in control.

An employee’s use of the internet for personal or trade union use should be of a reasonable level and should not be defamatory or offensive.

Monitor what is on the web about yourself. Type your name (in various forms) into several search engines.

Think “I do not trust email”

2 trillion email messages are sent a year. Despite this it is still not possible to verify that the “from” address is valid and actually sent by the person listed – criminals prey on this fact.

“Phishing” or “Brand spoofing” is a practice used to obtain credit card numbers, or other personal information in order to commit identity theft. This can be done by a number of methods including faking e-mails and creating websites similar to legitimate ones.

Be aware when using a credit or debit card to order anything online – only use reputable companies or sites that offer some verification of resellers (e.g Amazon, e-bay). If you are unsure do not proceed. If you wish to buy from an unknown

site then pay via pay-pal. Remember if it sounds too good to be true, it probably is!

Never use website links that are in an email as they can easily be fake. Instead, open up your browser and type in the website address you know to be correct. This simple step ensures you never get to a fake site or supply information to criminals.

Reputable companies will never solicit personal information via email – if in doubt phone them. The personal situation you share with your friend in confidence can easily be sent to millions of other email addresses years after it was sent. Ask Lucy Gao, Claire Swire or Richard Phillips (Google them!).



Personal Information

Take care what passwords you choose. Don't make it obvious. Avoid family names, addresses, hobbies and birthdays. Use a mix of letters and numbers, include punctuation also. Use a strong password for banking, use an easier password for email / everything else. Don't give students your personal e mail address, mobile phone number, or Instant messaging details, even if there seems like a good reason to do so – eg. project work over a holiday. Use school based e mail if you have to communicate with students electronically or set up a special e mail on a free service (hotmail/google).

At home use a firewall and antivirus which will prevent some malicious software, viruses and Trojans from entering your computer, ensure these update daily. Windows users should set "Windows Update" to automatic.

Exercise your option not to have your name published on the electoral roll.

Is the house where you live and its land line telephones identifiable through a telephone directory?



Your mobile 'phone

Don't phone students' homes or mobiles without using the code that withholds your number.

If you keep your phone switched off at school and the bluetooth disabled it will prevent blue-jacking which enables people to access your phone without your permission.

Don't model the use of phone cameras - this encourages students to do like wise and so they may become the victims. Don't allow students to video you or other students on their own cameras or videos even at the end of the school year.

Consider setting up your phone so that it withholds your number. Individual Service Providers will be able to help you.

- don't respond to malicious texts or emails
- save evidence
- report incidents





Cyber Bullying

Cyber bullying is 'the use of Information and Communications Technology, particularly mobile phones and the internet, deliberately to upset someone else'. It can affect staff as well as pupils. Schools should state in their anti-bullying and/or behaviour policy how they will address cyber bullying, including the bullying of staff. If at any time you are being targeted, talk to your manager or go to www.warwickshire.gov.uk/bullying for more information.



Don't be the victim!

Student teachers leaving university are frequently **unaware** of how new technologies can be abused.

What is amusing and entertaining amongst college friends can be used later to **ruin your professional career** before it has hardly started.

For help and advice visit:

www.thinkuknow.co.uk

Contact Details

If you are a victim of cyber bullying or are targeted please ensure you contact the ICT Development Service. Initially you will be put through to the Service Desk who will then pass on your concerns to the relevant team.

ICT Development Service Desk
01926 414100

This guidance is supported by the Trades Unions and Professional Associations within Warwickshire



In Support of Learning



ICT Development Service

