Telford & Wrekin Safeguarding
Children Board (SCB)

December 2014

Raising Awareness: Latest advice on the Safer use of Information Communication Technology (ICT) systems at home and in the workplace.

Introduction

You will be aware from the national media, that there have been a number of high profile cases regarding abuse of the Internet, mobile phones, e mail, social network sites such as Facebook and Twitter This can lead to Child Protection discussions and raises the issue of taking advice in terms of personal protection in the safer use of ICT.

At a local level this has been found to be no different, where there has been an increased caseload of allegations against individuals, especially those that work with children in their occupational status, some through sheer naivety. The situations that people find themselves in can be distressing, but this may have been averted at an earlier stage with some common sense guidance and tips for the protection of all computer users. Even if your work may not be with children this advice is useful to note.

Overview-The Safeguarding Children Board (SCB)

The Safeguarding Children Board is a multi agency arrangement which replaced the Area Child Protection Committee's. The Board members represent their organisations at the most senior level and were established under HM Government's "Working Together to Safeguard Children".

The SCB has a number of senior ranking individuals as members in organisations across multi agency disciplines. Every Local Authority has to have a SCB in place. Officers of the board are charged with investigating allegations against all staff where there may be child protection concerns, these Officers are known as the Local Authority Designated Officers (LADO).

Although the SCB is specifically aimed at children and their welfare, the SCB feels it has a duty to provide guidance to all ICT users, This is especially true in regard to self protection in the ever changing world of technology, in or out of work, whether child or adult..

Action

After discussions about recent cases at a local level with the School Community, Telford & Wrekin Council Officers, Union Officials and Officers from the Safeguarding Children Board, some guidance was produced specifically for schools back in 2007 and 2011.This new guidance is for general use but does reflect those that may work with children and young people but it is felt that everyone should be aware of this advice.

Safer use of Social Networking-Internet-Phones-Email

Using New Technology - Hints and Tips for staff working with children and young people

Read this, it might be helpful even if you don't …

Social Networking hints and tips

Social networking sites are excellent ways to stay in touch with friends and share photographs, comments or even play online applications such as chess or word games. However, they are also designed to enable advertisers to target you and entice you into buying goods and services based on the 'profile' information you reveal, they are often set for all to see! Be web savvy!

- Social networking sites, such as the currently most popular "Facebook", **have a range of privacy settings**. These are often set-up to 'expose' your details to anyone. When 'open' anyone could find you through a search of the networking site or even through a Google search. So, it is important to change your settings to "Just Friends" so that your details, photographs etc., can only be seen by your invited friends **(please see the attached example on setting to privacy, also the attached Facebook Checklist).** Please note that other providers have similar settings so that access is restricted.
- Have a neutral picture of yourself as your profile image. Don't post embarrassing material. Be careful what you post! Increasingly companies and organisations "trawl" open Facebook profiles before they interview or appoint!
- You do not need to accept friendship requests. Reject or ignore them unless you know the person or want to accept them. Be prepared to be bombarded with friendship requests or 'suggestions' from people you do not know.
- Choose your social networking friends carefully and ask about **their** privacy controls.
- Do not accept 'friendship requests' on social networking or messaging sites from students, pupils or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.
- Exercise caution – for example in Facebook if you write on a friends 'wall' all their friends can see your comment – even if they are not your friend.
- There is a separate privacy setting for Facebook groups & networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile. Check it out!

- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.
- If you wish to set up a social networking site for a school/youth project create a new user profile for this, do not use your own profile.
- If you or a friend are ‘tagged’ in an online photo album (Facebook, Flickr or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.
- You do not have to be friends with someone to be tagged in their photo album.
- If you are tagged in a photo you can remove the tag, but not the photo.
- Never knowingly give permission for students to take your photograph with their own mobile phone
- Photo sharing web sites may not have privacy set as default.
- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.
- Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a ‘web crawler’ and it will always be there. Archives of web content are stored on sites like the “WayBackMachine”.
- Think about your internet use, adults are just as likely as children to get hooked on social networking, searching or games. Be aware of addictive behaviour!
- You will not be able to remove yourself completely from the Internet. 192.com has all the English electoral roles and for as little as £9.99 your personal information can easily be found by a stranger.

Wider Internet hints and tips

- Never tell anyone your password.
- In the workplace and in all Telford schools, ICT systems are monitored. If you are surfing the Internet and visit inappropriate sites it will be recorded. If you visit inappropriate sites, this could lead, in the worst cases, to a criminal prosecution and disciplinary action. For avoidance of doubt please acquaint yourself with your work Corporate Information Security Policy (CISP) and Social Media Policy. Also if sites are visited inadvertently make your Senior Management Team aware and seek advice from your ICT Team.
- Be careful how you choose passwords, most are very predictable. It is easy to find personal details online that might give password clues. It is recommended that you include capital letters, lower case letters and numbers – avoid birthdates, names, pets, addresses etc. It is best to avoid any word found in a dictionary.
- Be careful when form filling online…., do you know who the data is for? Only answer ‘required ‘questions, do not just give out information because you have been asked for it.
- Never verify banking details online.

- When you need to use a ‘name’ online consider what name you use. In a professional context you would probably use your full name, but in other contexts you may decide to use an alias to protect your identity. If so make sure it is appropriate.
- If you create a family tree and post it on the Internet, make sure your tree is set to private for anyone living or recently deceased (last 50 years). The information posted would be enough for someone to steal your identity and probably guess passwords and common security questions.
- If you get a phone call or an email from someone asking you to confirm personal details, (unless you are expecting the contact), do not give out any personal information.
- Popup adverts are often a nuisance. Close them carefully as a ‘close’ button will often lead you to more advertising as the ‘X’ might be a graphic.
- If you get an email or popup offer that seems too good to be true it probably is! Watch out for online cons – it is like online door step selling.
- If someone sets things up for you at home, make sure you change your password immediately. Someone with your username and password could impersonate you.
- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name, sites cannot work from a hunch.
- Cookies are not necessarily a bad thing. They save your surfing information and speed-up access to sites. However, if someone else has been surfing ‘adult content’ on your computer, the stored cookies may mean you get ‘adult pop-ups and adverts’.
- Use legal sites for downloading music, films etc., such as iTunes.
- File sharing sites are not illegal but sharing of copyright material is. Downloading of illegal music and film downloading also leaves you at a huge risk of viruses. Even if you subscribe to a file sharing web site, such as Limewire, it does not mean that your downloading becomes legal.
- You can get Internet access from many games consoles and some MP3 players. Games with multiplayer features are often labelled as ‘net play’. This means that you are playing with strangers online – the risks here are the same as for social networking, chatrooms and messengers.
- Applications like Skype and iplayer need bandwidth and can slow down the internet, particularly if you use a 3G mobile stick. Full screen iplayer could use up your allocation and your service may be ‘throttled’ - meaning you can only do some basic text work, searching and emails, but picture and video will not be possible.
- When you log-into a web site, unless your computer is exclusive to you, don’t tick boxes that say ‘remember me’.
- Don’t leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.
- Don’t give your username and password to anyone such as to a supply teacher / temporary member of staff – make sure your school has a guest login for visiting staff.

Your school or work laptop (or other equipment) should not be used by friends and family.

If you work with young people:

- Try to provide pupils with direct links embedded into ‘pages’ in a document, Learning Platform, or interactive whiteboard resource etc.
- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even the most innocuous term can bring up adult material.
- Use child-friendly search engines with younger pupils. Older young people will use a variety of search engines at home, you are a role model for them in good use of a search engine. Look for opportunities to teach young people how to use search engines.
- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.
- Watch YouTube (or any) videos before you use them in the classroom.
- If you use a YouTube (or any) videos, find out how to embed it using the ‘Source’ rather than a page link, as that exposes pupils to other content. You will also need to uncheck the box which allows the embedded video to suggest related videos.
- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.
- If you want to use a clip download it (if legal & copyright allows). Otherwise it might not be there next time you look for it.
- If you use your own equipment in school (such as cameras or laptops), ensure senior leadership have given you permission and make sure that school files (photographs etc) are downloaded and stored in school, not at home.
- Do not take stored pupil photos or information home. If for any reason you need to ensure you have senior leadership’s permission, and ensure it is on an encrypted device.
- Remember that if you leave a computer running and leave the room it can be tampered with by students and may leave you open to exploitation. Wherever possible, good practice would be to lock the computer by pressing Ctl-Alt-Del and press K for the duration of your absence
- Video Conferencing – you can be broadcasting without realising it, if you have VC in your classroom make sure it is switched off after use and that the camera is turned away from the class.

You need to be a role model for copyright. Make sure you use multimedia resources appropriately, don’t just ‘grab stuff’ off the Internet. Use the copyright images from the NEN, Learning Platform or other sites your school / LA has advised you of. You cannot show DVDs in school, although it is safe to use film trailers. But, make sure you download the right version, as there are can be more than one film trailer, including trailers for ‘adult versions’ of blockbusters.

Email hints and tips

- Keep all your work and private transactions separate. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.
- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.
- If you get an email from someone or a company that you have never head of and it asks you to reply to unsubscribe, don't. By unsubscribing you will verify that you exist. Just ignore the email. If they carry on emailing use email rules to block the sender.
- If you get emails that offer you money making schemes (e.g. the 'Nigerian email'), Russian wives, pharmaceutical products and body part enhancement don't be upset, you have not been personally targeted, this is spam and junk mail.
- Webmail is useful but insecure, and your email address is easily passed on.
- If you get spam or junk mail it does not mean that someone has 'hacked' into your email; people get email addresses in different ways, it might be a software 'guess' – a programme generates lots of possible emails and sends out millions of emails knowing that statistically some of them will be real. Software also searches web sites for email addresses and harvests them.
- Only open Email attachments from trusted sources, you won't get a virus from the initial email text, but it may be contained in an attachment.
- If emails from friends or acquaintances start to become unsuitable – say something before you receive something really problematic.
- Don't give out private email addresses to students and pupils.

Phone hints and tips

- Don't give out your mobile number or home number to students, pupils or service users, unless there are exceptional reasons to do so *(see below).*
- If you have a Bluetooth phone do you know if Bluetooth is turned on or off? If it is on is there a password? Open un-passworded Bluetooth means anyone else with Bluetooth in range can read the content of your phone or device.
- Many hand held games consoles have wireless and Bluetooth and can be used to make contact from 'stranger' devices within range.
- Be very careful what you store on your mobile phone, if it is taken by anyone they may get information which could be embarrassing in a number of ways

Are there any circumstances where it may be considered that legitimate use of ICT interaction with young people and service users is acceptable, through my work and in exceptional circumstances outside of work?

It is recognised that there may be exceptional circumstances where it is acceptable within or outside of work to have legitimate contact via ICT methods. Within the school network this is closely monitored but all staff should, if they have to, liaise via work based equipment, this shows transparency. However, the balance, proportion and culture has to be right and no one would wish a child or service user to come to harm because of bureaucracy and a lack of common sense in decision making and not “doing the right thing”.

It may also be considered that other exceptional circumstances could be considered appropriate, these include;

- Outdoor Trips, especially outdoor pursuits and those abroad. It would be entirely appropriate and for the duration of such activities for children to be safe and in contact with those leading them

- Children or service users who are classed as “gone missing” should always be reported through to the Police without delay. However, on Police advice and only on instruction by them on a case by case basis, there may be exceptional circumstances where staff could be judged to be more appropriate to make personal contact, this would be exceptionally rare. For example this could be considered where the Police feel their presence may inflame a situation.

- Youth Offending Service, Health, Sexual Exploitation, Therapeutic and Social Care Teams sometimes manage appointments by text messaging, where often this is the most appropriate way that young offenders, patients and service users engage and manage to keep appointments

- Professional judgement, where in the absence of the need of direct Police intervention, immediate action is necessary for the immediate safety or concern of any child, service user or those people around them.

Keeping legitimate contact real in the ICT world

Advice for all is to be accountable for your actions, including some useful tips to follow;

- Where possible use work based ICT Systems and processes
- If personal ICT Systems are used clearly account for that use
- Clearly action your rationale and reason as to “why”
- Document your actions and show transparency
- Be mindful/sensitive of “tone and content”
- Be aware of professional boundaries and recognising early indications of imbalances in that relationship
- In what context did the exceptional; circumstances occur, and
- If Communication is to be made within your organisation, then make that clear to your line manager for endorsement at the outset

Facebook-Briefing note on setting your status to privacy

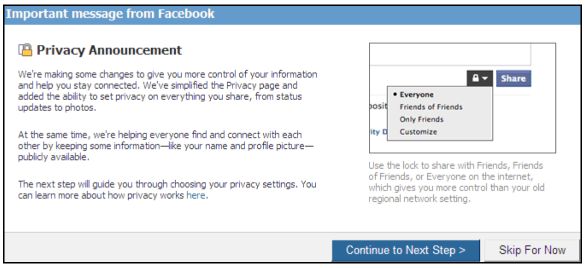
This briefing note is not aimed at the use of Facebook in school or the workplace, ***but has implications for e safety and privacy for all Facebook users*** – adults and young people.

Facebook are currently directing all users to review their privacy settings through an on screen message window.

Why is this a concern?

- The process may lead Facebook users to widen access to their personal information from **friends only** to **everyone** without realising it.
- We are aware many pupils use Facebook, including young people at Primary schools. The age restriction for Facebook is 13 but many young people use Facebook with parental permission so we would not recommend asking Facebook to routinely remove all underage profiles unless there are issues such as cyberbullying or inappropriate contact or posting.

What does the Privacy settings review look like?



Important message from Facebook

Privacy Announcement

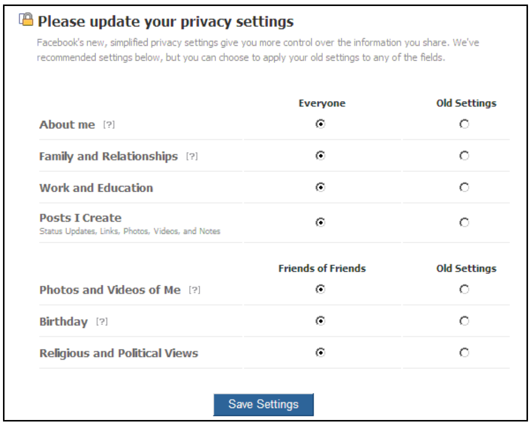
We're making some changes to give you more control of your information and help you stay connected. We've simplified the Privacy page and added the ability to set privacy on everything you share, from status updates to photos.

At the same time, we're helping everyone find and connect with each other by keeping some information—like your name and profile picture—publicly available.

The next step will guide you through choosing your privacy settings. You can learn more about how privacy works here.

Use the lock to share with Friends, Friends of Friends, or Everyone on the internet, which gives you more control than your old regional network setting.

If you say **continue to next step** you get the screen below, notice it has suggested opening the profile up to everyone – the temptation is to just select **save settings** and as a result open up your privacy to everyone.



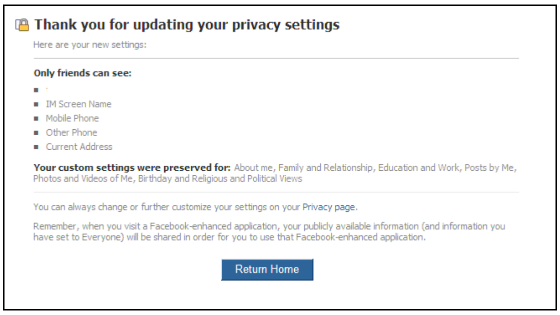
Please update your privacy settings

Facebook's new, simplified privacy settings give you more control over the information you share. We've recommended settings below, but you can choose to apply your old settings to any of the fields.

	Everyone	Old Settings
About me [?]	●	○
Family and Relationships [?]	●	○
Work and Education	●	○
Posts I Create Status Updates, Links, Photos, Videos, and Notes	●	○
	Friends of Friends	Old Settings
Photos and Videos of Me [?]	●	○
Birthday [?]	●	○
Religious and Political Views	●	○

We strongly recommend users to:

- Keep old settings
- Only share with Friends
- Do not share with everyone



Thank you for updating your privacy settings

Here are your new settings:

Only friends can see:

- IM Screen Name
- Mobile Phone
- Other Phone
- Current Address

Your custom settings were preserved for: About me, Family and Relationship, Education and Work, Posts by Me, Photos and Videos of Me, Birthday and Religious and Political Views

You can always change or further customize your settings on your Privacy page.

Remember, when you visit a Facebook-enhanced application, your publicly available information (and information you have set to Everyone) will be shared in order for you to use that Facebook-enhanced application.

To check your privacy settings

- Log into Facebook
- Selects settings from the top bar (right hand side)
- then privacy settings
- profile information

If you have concerns – reporting issues to Facebook

Facebook will only follow up concerns if their terms and conditions have been breached

- Email from a school email address only to abuse@facebook.com
- Include the URL of the profile you are reporting – the name of the person is not sufficient
- State why the profile/page breaches terms and conditions (http://www.facebook.com/terms.php)
  e.g. pupil is under age 13, the profile is an imposter etc.
- Put your contact information, including your job title etc.