

## Community Cyber Ambassador Newsletter (Vol 5. August 2017)



### Creating a safer Cambridgeshire

Online networking has revolutionised the way we communicate and interact with others and for many users, it has become a way of life. It gives us the ability to talk one-to-one and/or to large groups of people all at once and share our experiences and in many ways it has replaced traditional methods of communication like telephone and email.

The term social networking can be applied to many **websites and apps** and with new sites springing up every day there are far too many to mention individually in this newsletter. Below is a description of some of the most popular types:

**Blogging** – A blog, short for web log, is a website that is regularly updated with new posts, similar to a diary. Services such as Blogger, WordPress and MSN Spaces have made it easy for private individuals and companies to set up their own blogs. Vlogging is similar to blogging but instead of writing updates on a website the author will create a video log.

**Chatrooms** – these are virtual places or spaces on the internet where people can get together and ‘talk’ using text. Some chatrooms use specific programs to access and use the facility while others are built into websites, including social networking sites. These large online

### *Being a responsible cyber citizen on social media*

We all know what is socially acceptable in the real world but did you know that these rules also apply when we go into cyber space? Some basic rules or “netiquette” can be found below:

- Remember the Person: Behind every screen, post and/or avatar there is a human being with their own thoughts and feelings.. Being anonymous online should not influence how you communicate with others. Think if you were face-to-face with that person would you say out loud what you are posting/writing online.
- Laws that govern society in the real-world also extend to our actions in cyberspace. This includes harassment, bullying, copyright regulations and privacy.
- Think more real life. We behave differently in different environments i.e. with friends at a social gatherings or with peers at work or inside school. The same is true online and you should consider whether your comments and pictures on some sites may be inappropriate for others i.e. Facebook vs LinkedIn. Pay attention to your word choices and the truthfulness of what you write as other users will take this as their first impression of you.
- What goes online, stays online. Even if you delete a post or picture, it could have been shared, copied or saved a thousand times. Think about the type of language you use.
- Disagreements happen between people all the time in the real world and online is no exception. The difference is online these exchanges can linger as there is a record on the net. If you find a discussion gets heated online, give your opinion using neutral language and if it gets really heated

communities mean that it is more likely that you might come across anonymous strangers and unfiltered and/or unmoderated discussions.

**Instant Messaging (IM)** – Instant messaging (IM) allows you to ‘chat’ in real time over the internet in a similar way to mobile phone text messages. Advanced systems allow webcam and voice communication. The main systems are: Windows Live Messenger (formerly MSN), Yahoo! Messenger and AOL Instant Messenger. Instant messaging can be great for staying in touch with friends but, like email, it carries risks.

**Internet Calls** – Also known as Voice over IP (VoIP) or internet telephony services these services are convenient and very inexpensive and use your internet connection to transmit voice calls. These services can be supplied by companies to just make calls but some, like Skype, can also enable users to invite and form contacts, create profiles, make video calls and share files.

While social networking can open up new opportunities and friendships for many it can also leave people wide open to some kind of abuse – be it financial or personal- especially where the person who you may be communicating with is unknown to you and you can’t easily see them.

The web is an open forum and in order to make sure that you stay safe it is important to remember the following when using social media:

- **Never** disclose private or personal information when using social networking (including information about friends and family). This could help criminals to commit further crime on and offline and might cause trouble for yourself or your friends and family.
- Be **wary** about who you invite or accept invitations from. **Never** be pressurised by a new contact into taking a conversation outside the social media site or offline until you really get to know them and **NEVER** send money or personal details to someone you have only just met online.
- **Be** careful about clicking on links in an email, social networking post or message if you were not expecting it or it has come from someone you don’t know.
- **Think** very carefully before being persuaded or harassed into changing your basic beliefs or ideologies, or adopting an extremist stance.
- **Frequently** check your privacy settings on your social media accounts and don’t presume they will stay the same. Setting these gives you control of what you share with whom.

More advice on using the different social networking sites safely can be found at [www.getsafeonline.org](http://www.getsafeonline.org).

The UK Safer Internet Centre has produced safety checklists for some of the biggest sites including Facebook, Twitter, Instagram and Snapchat to provide advice and guidance on how to set privacy settings on some of the most popular social media accounts but it is also good to check the social networking sites’ own online safety pages.

Next month’s newsletter will focus on safe devices