



- Set limits on when they can use the computer and for how long.
- Encourage them to come to you if anything online makes them feel uncomfortable or threatened.
- Make it very clear that they must not give out personal information without your permission. In particular, addresses, phone numbers, school details, passwords or pictures.
- Warn them to be careful about giving away their email address in chat rooms or when registering for sites.
- Forbid them to meet anyone in person that they encounter online without your consent and without a responsible adult present.
- Agree what types of sites are permissible and which are not; for example you may make a policy of not allowing them to use un-moderated chat rooms or to use file sharing programs.
- Restrict their ability to download software, music or other files without your permission. (Big difference between iTunes & File Sharing Systems)
- Agree whether (or not) they are allowed to spend money online. Although you might not give them your credit card, if you have already stored your details at an online store it may be easy for children to spend your money if you don't take steps to limit their access or agree ground rules.
- Explain what viruses and spyware are, what you are doing to prevent them and ask them to come to you if they get an alert while online.



- Research age-appropriate internet sites that you can suggest to your children.
- Adult to set up email and password, to allow for access, updating or changing when need arises.
- For all sites that require email log an adult should setup email and password, to allow for access, updating or changing when need arises.
- Remember your computer can be set up to allow users to automatically log in. Email username should not include identifiable features such as (amy_14_leeds).
- Messenger service (MSN or Yahoo) to be set up so as to save chat history, and should be periodically checked (for any offline messages).
- SNS (Social Networking Service) profiles to be created by adult so as to be in control of password, to allow for access, updating or changing when need arises. Computer can be set up to allow user to automatically log in. Allow membership to just ONE site.
- SNS profile not to include image of user on home page (Un 16). Profile to be set to private, however, remember some SNS do have facility to show who is online. Password to be kept by parent / guardian to allow for access, updating or changing when need arises. Remember computers can be set up to allow user to automatically log in. No personal details on site.....Email /mobile /address / school / clubs / age.....etc



- Parent / Guardian to become members of the same site, either with or without correct details, photograph to be included. Add son / daughter as friend / contact, and they must accept you.
- Parent / Guardian to add their profile and photograph to home page of son / daughter, for all child's contacts to see, perhaps with heading 'My mum / dad who sometimes comes on as me to check.....etc'.
- Every 2 -3 weeks log on as the younger user and make it known that you are not them and are there to check.
- Chat facilities, Web Cam Chats, File Sharing Systems should NOT be used, even if they state they are for children only. The users are only electronically verified and so anyone can join.
- Consider limiting the amount of friends son/daughter allowed to invite / accept dependent on age; eg (11-13 yrs = 30 contacts) (14 yrs = 40 contacts)(15 yrs = 50 contacts)(16 yrs = Unlimited but monitored)
- Please also see our **Huddl Social Media Best Practice** and **Huddl Safe App Guide** in our resources section of our website.
- Useful links for further advice:
 - www.internetmatter.org
 - www.besafe-online.co.uk
 - www.saferinternet.org.uk/advice-centre/parents-and-carers
 - www.nspcc.org.uk/preventing-abuse/keeping-childrensafe/shareaware/
- Apps to keep kids safe:
 - www.childline.org.uk/toolbox/for-me/