E SAFETY GUIDANCE

E Safety is Everyone's Responsibility

Every member of staff has a responsibility to reinforce the message about staying safe online. If a student does speak to you about any 'cyber' issue, it is policy that this is reported to Richard Potter to follow up.

For further support, visit http://ceop.police.uk/. CEOP—Child Exploitation and Online Protection provide good materials for tutor time/ lesson discussions or preparation for assemblies regarding online protection

Staff and students should be reminded that any online problems/ bullying can also be reported direct to CEOP/ the Police by using the following symbol, on many social media sites:

NOTE: For arguable reasons, some sites, such as FACEBOOK, only allow their own reporting mechanism NOT CEOP

The have been a number of apps which all parents, staff and students need to be aware of. These have been added to the E Safety page on the school website. However for clarity the top concerns are:-

- **YIK YAK**
  - An app that allows anonymous messaging to anyone within a mile and a half radius. Clearly, such an app that raises a number a number of e safety / child safety concerns. Please report any use of this app to Richard Potter / Wendy Crick
- **ASK FM**
  - Ask.fm is a social networking website that enables users to ask and answer questions. It has become popular with young people and there are millions of users around the world. Partly because of the ability for users to post anonymous questions, the site can be abused and used for.
- **SNAPCHAT**
  - Images posted between people, normally friends. However these images disappear after a few seconds. However NOTHING is ever DELETED ONLINE. Additional screenshots can easily be taken and reposted.
- **OMEGLE**
  - **STUDENT'S SHOULD AVOID** Omegle is a website that allows you to chat with random strangers. ASL (age sex location) is a common text style message when talking to strangers on this site.
- **KIK**
  - KIK is effectively a free texting service, consequences are there is a possibility of cyber bullying
- **VINE**
  - Vine is a video sharing service and app that allows users to make 6 second videos and share them online. These can then be screenshotted and used as a potential source of cyber bullying.
- **Tinder**
  - Is an online dating app which can pick up users locations if location services are switched on. This app should be avoided

Bottom Line Message to Students

Never continue an online conversation if you are uncomfortable, **JUST REPORT IT**.

If possible any issues that they feel could be indeed cyberbullying should be screenshotted where possible as evidence.

Profile images should not be 'selfie' style images, images from a distance, or images of half a face protect your personal online identity.

Further guidance and advice can be found on the Sir Harry Smith website

http://www.sirharrysmith.cambs.sch.uk/

General Guidance

Your professional reputation is part of your current and future career so managing your online reputation is essential. Anything that you post online is potentially public and permanent even if you have used privacy settings on your account. On social media friends can repost or comment on your posts which means others to whom you have not given access may view your comments. (ASCL, Social Media Guidance, 2014)

Reminder Strictly No Students as Friends

Please consider any 'friends' that you accept online. The Sir Harry Smith Community College policy states that you should not accept any students on your personal friends list. This will help to prevent any **unwanted contact**, or attempted unwanted communication.

Any departments operating, or considering a social media page must ensure that they make their pages known to Richard Potter to ensure that these pages are linked to the school's website; supporting their validity/ credibility. Moreover, departments must be following the NO STUDENTS as social media 'friends' rule. Pages should be designed so that students can access a meaningful learning forum.

Most common sites departments have used are:

- YouTube
- Twitter
- Facebook

If you require any training or advice on such matters, please email reception@sirharrysmith.cambs.sch.uk

Preventative Measures

Top Ten Privacy Settings

1. Friends only ensure that only friends are able to see your profile in Facebook. Friends of Friends is not secure. If you don't know them, they should not be able to view information about you.
2. Have more than just one friends list close friends could have different access to images, posts, or tagged images. Perhaps a different privacy settings for 'Friends' and 'Family'.
3. Ensure that friends cannot check you into 'places' without your permission- keep your location secure. In 'customise settings' ensure that you have disabled '.

4. Remove yourself from Facebook search results—this will mean that it is not possible to search for your name in Facebook.
5. Remove yourself from Google. A lot of information from a range of social media sites ends up on Google. To ensure that you are not included in the information accessible by search engines, ensure this option is ticked.
6. Avoid others viewing images you are tagged in that you don't want them to see. Allowing this option will ensure that any images that you are tagged in will not appear. Only YOU should be able to control the images that you are tagged in.
7. Always make contact information private.Often students display their mobile or an email. This is dangerous, or, at best, ill considered, leaving you open to unwanted communication.
8. Avoid embarrassing wall posts— Ensure that the option in the privacy settings is enabled to ensure that only you control what is posted to your wall.
9. Avoid allowing other applications to have the ability to gain access to information / personal biography of you. Make sure that others cannot draw inferences from what you write on social media, or indeed what you search for. Instant personalisation traces your searches or social media activity to target you for marketing purposes. To avoid any annoyance, turn of sending data to other applications/ websites.
10. Consider what you post. Once information/ images/ data is on the internet it is virtually impossible to remove it.