All Saints School's Guide on being safe and responsible online

The Internet and the increasing number of digital devices and applications you use to connect to it are an integral part of your daily lives. However, despite all these opportunities to stay in touch with friends, education and entertainment, there are online risks as well which can lead to harm.

Here are some of these risks explained and advice on how to keep yourself safe and to protect your online reputation.

Cyberbullying

Cyberbullying is bullying that occurs online, often through writing hurtful things through emails, instant messaging, text messages, posting derogatory messages on social networks or posting embarrassing photos or videos.

It could be even more hurtful than other type of bullying and more difficult to stop.

Advice on responding to cyberbullying:

- **Don't reply to the bully.** Bullies often want to get a reaction from their victims. If you ignore them, they may lose interest.

- **If possible, block messages from the bully.**

- **Keep all emails and other messages that the bully sends.** You may need to use these as evidence at some point.

- **Report the bullying to a parent/guardian or a trusted adult.**

At All Saints we have a zero tolerance to any type of bullying, so if yourself or any of your friends are being bullied, **please report it to Mr. Poddington (Designated Safeguarding Lead), your Head of the Year or any teacher you may prefer.**

Sexting

Sexting is sending sexually explicit photographs, videos or messages via mobile phone or social media. Can include "nudes", "underwear shots", "dirty pics" or rude text messages.
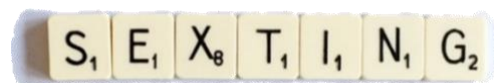
Once you have posted something online, you have lost control of it. It could be resent, duplicated, copied and shared with a large number of people.

Even if you feel you are under peer pressure or somebody is daring you into sending a sexually explicit image or text **stop and think** about the potential social humiliation of this being shared with the whole school or wider community.

Please watch this video about the **consequences of sexting**:

https://www.youtube.com/watch?v=V4DenkTtZpg&t=1s

Advice on sexting:

- **Don't do it, under any circumstance.** Think of the potential humiliation and protect your online reputation.

- It is illegal to possess, take or distribute sexual images of someone who is under 18, even if that person is yourself. **Delete any such images or videos immediately.**

- **In the worst case, report it and try to remove it as soon as possible.**

Report it to Childline: https://www.childline.org.uk/

or make a report directly to the Internet Watch Foundation (IWF).

Online grooming

Online grooming is when someone builds a relationship with a young person online because they want to trick them or pressure them into doing something that may hurt or harm them.

The consequences of online grooming could be very severe, so please if someone online is making you or a peer uncomfortable, then tell an adult you trust like a parent, guardian or a teacher.

Top tips on preventing online grooming:

- **Limit contact online to people you know and trust and use privacy settings.**

- If someone online is pressurising you or a friend, making you uncomfortable or asks to meet up, **speak to an adult you trust straight away.**

- If you are in contact whit someone you don't know in real life**, do not share personal information online such where you live, go to school or photos/videos of yourself.**

- **You can report any suspected grooming to the police, using the "report abuse" button.**

Privacy and identity theft

Any individual using an online digital platform such as social media apps or online games are at risk of having their personal information, credit cards details, logging details to social networking accounts stolen. Some criminals are using social media sites as hunting grounds for finding private information which they can then exploit.

The consequences of having your identity or personal information stolen could be a financial loss or a loss of online reputation which may then affect you in the future when applying to University or in your future career when applying for jobs.

Please watch this video about the **consequences of identity theft**:

https://www.youtube.com/watch?v=CJ40tAm8cTE

Tips on keeping your private data secure:

- **Take control of your privacy:** think carefully about what you want to share online and what you want to keep for yourself.

- **Respect the privacy of others:** don't share information or photos /videos of your friends or others without their permission.

- **Minimise the personal data you share:** delete the social media accounts or the online gaming accounts you no longer use, choose "reject all" when asked about cookies on different websites

- **Use the privacy settings for all the social media sites or online gaming accounts or apps you may use online.** Manage who can see you're the things you share online and tests the settings to see if they are working.

Here are some useful websites to help you:

- Safety and privacy settings tips for **Twitter:**
https://www.lifewire.com/staying-safe-on-twitter-2487775

- Protecting your privacy on **Instagram:**

https://www.theverge.com/2020/2/27/21154221/instagram-privacy-how-to-stories-posts-settings-tags-ads-blocking

- Using the ghost-mode on **Snapchat:**
http://www.bbc.co.uk/news/technology-40509281

If you are unhappy or uncomfortable with any interaction you had online or you have any concerns please talk to Mr. Poddington (Designated Safeguarding Lead), your Head /Deputy head of the Year or any teacher you may prefer.

To report peer on per abuse please contact Childline:
https://www.childline.org.uk/
Report serious incidents to the police (CEOP) :
https://www.ceop.police.uk
or if in immediate danger call 999.