



# Student Online Safety



## Looking out for your wellbeing

### When online it is important to consider all aspects of your safety and your wellbeing:

- Ensure you take regular breaks – spending large periods of time online can have both physical and mental impacts. Using wellbeing settings and apps. Social Media Platforms such as Tiktok now have a screen time function which allows users to manage the amount of time they spend online/social media. Most apple and android devices now have a function for digital wellbeing, which allows you to track the length of time spent on certain apps/internet and allows you to set screen time, app managers, alongside sleep mode, and reminders for ‘me time’ promoting positive wellbeing and self-care;
- Isolation, it is easy to feel isolated online, particularly if you don't have your normal support network to access in person. The University procured Umii in 2020 to help students avoid feeling isolated and to support students making new friends:

<https://umii.app>

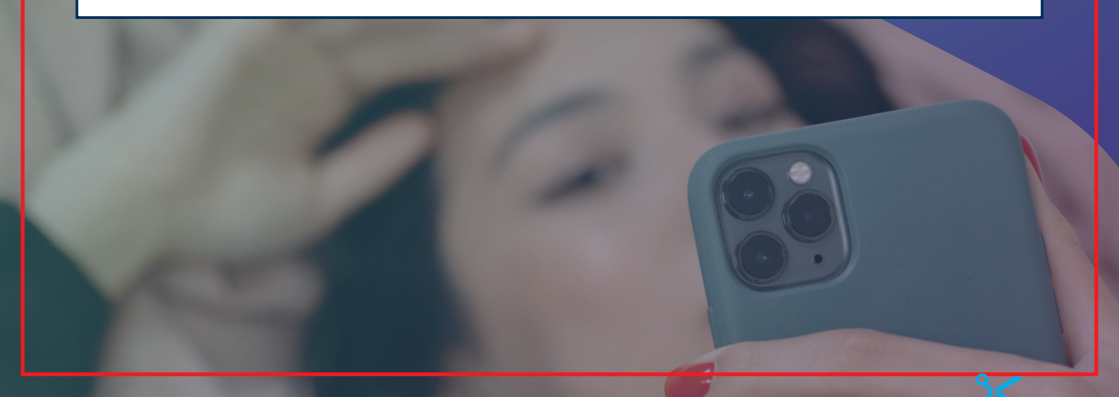
- Social media and privacy: Social media is never private, and posts you make now can be seen in the future even if you think you have removed or hidden these. Many employers now look at the social media accounts of applicants. Be careful with what you post, a fun post shared amongst friends could be seen by potential employers. The University has further guidance on the use of Social Media:

<https://www.bolton.ac.uk/student-policy-zone/>

- Keep yourself informed of security risks and IT phishing scams to protect yourself, your work and your personal information when working online. Check out the <https://www.getsafeonline.org> website for guidance;
- The internet is a great source of information however not all information is reliable, check out <https://www.snopes.com> or the [https://www.bbc.co.uk/news/reality\\_check](https://www.bbc.co.uk/news/reality_check) to find fact from myth.

## Basic measures to stay safe online

- Check privacy settings on social networking sites and limit the amount of information you supply;
- Google yourself frequently to check your digital footprint, some antivirus software now can assist you in seeing what information about you exists online;
- Use secure and unique passwords and use more than one password;
- Be aware of geolocation and tagging on social networking sites, turning off location settings can help protect your privacy;
- Keep your antivirus software up to date;
- Many laptops and webcams now have lens covers, cover your webcam when you are not using it;
- If you receive an email/text message from a stranger or a suspicious email that doesn't look genuine don't open it or click on any links;
- If you believe that your smartphone or computer has been hacked or compromised, stop using it immediately and get advice from a reputable computer repair shop;
- Be careful who you chat to, if somebody you don't know adds you as a friend, ignore them and delete their request;
- Don't share personal information like your address or phone number with somebody you don't know. Also, be mindful with what information people can take from photos you may share, what's in the background? Is there anything that might identify where you live?
- Check to see if your email has ever been compromised in a data breach using Have I Been Pwned: Check if your email has been compromised in a data breach <https://haveibeenpwned.com>
- Look for the padlock symbol before entering private information such as passwords or payment details, the padlock symbol is normally visible in the address bar and should show after the web address or 'https' in front of the web address in your browser.



## Social Media

Remember, what you post on social media is never private even if posted to a closed group, members of the group can always save and/or share your posts with people you wouldn't have shared information with.

It is very easy to post something to the world. Social media is not a place to let off steam or vent frustrations.

### Before posting something, take a moment to think:

- “Would I say this to the person’s face?”
- “What would I think if I saw this post on the internet?”
- “How might my current/future employer consider this?”
- “How would I feel if someone posted this about me?”
- “Could I be committing a criminal offence?”
- “What will my friends and family think?”
- “How would I feel if someone read about me posting this in the media?”

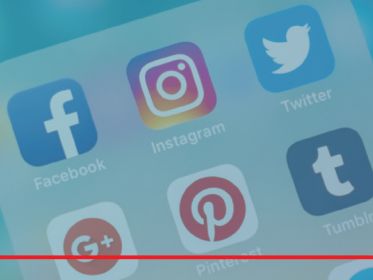
### Remember when using Social Media:

- Not everything you see is real, people don't always share honest opinions and or thoughts online;
- Pictures may be edited, staged or planned to look as good as possible;
- Take breaks, spending long periods of time on Social Media may make you feel worse, limit your time to 10 mins, social media can become an obsessive behaviour, detox and take a break from using social media.

For information on the University Social Media Guidance please visit:

<https://www.bolton.ac.uk/student-policy-zone/>

Social Networks



## Online Communities

Online communities can be great for getting help with lots of different things. But sometimes it's hard to know if an online community is making things better or worse.

Sometimes people go on websites which promote anorexia, bulimia or self-harm. This could be because they feel people in their life don't understand what they're going through.

However, harmful online communities can change the way you see life – even if you don't want that to happen. It can also trigger thoughts and emotions that may be harmful.

Ask yourself is a community helpful or making things worse? Leave communities that are having a negative impact.

If you need help and further support for your mental health and wellbeing needs, it is helpful to talk to a trained health care professional such as your GP, who can signpost or refer you to local support services. You can also seek support from the University's Life Lounge service which offers mental health and wellbeing support to all current students. You can find out more information including how to complete a self-referral via the following link:

<https://www.bolton.ac.uk/student-life/student-support/life-lounge/>

## Sexting/Sextortion/Revenge Porn/Blackmail

Sexting is a term used to describe the sharing of intimate images or videos with another person sometimes it can also be referred to as sharing of sexual, naked or semi-naked images videos, or sending of sexually explicit text messages. This content can be anything from texts, partial nudity photos right up to sexual images or video. Very often it is between partners, but can be between groups and can use a whole range of devices, technologies and online spaces. The most common ones are by text, private message on social networks or apps such as Kik, Oovoo, Instagram or Skype.

Sexting is very risky and can be very dangerous and damaging. There are lots of reasons you might want to send a nude. But if you're not sure whether you should or you're being pressured by friends, it can help to talk to someone you trust about what's happened. Remember once you have sent such a message you don't know who it may be forwarded to or where it could be uploaded.

Sharing nudes, videos or sexual messages with someone who doesn't consent to receive them can be illegal and you could be prosecuted.

### **If you've shared a message or picture with someone who doesn't want it:**

- Apologise about what you've sent;
- Stop contacting the person if they don't want you to talk to them;
- Don't pressure the person to send images or messages back;
- Talk to someone you trust about what happened, you can get advice from the Life Lounge.

### **If you've sent a nude and you're worried about what might happen, there are things you can do:**

- Ask for the message to be deleted: Explain that you're not comfortable with them keeping the picture and ask them to delete it;
- Don't reply to threats: if someone is trying to threaten or blackmail you don't send more photos. It can be scary, but it can help you to keep in control;
- Talk to someone you trust: Talking can be scary, especially if you're being threatened but it can also help you get support and stay in control;
- If something goes wrong: having a nude shared by other people without your consent is against the law and it isn't your fault. If you're struggling to cope or you don't know what to do, talk to the Revenge Pornography Helpline.

<https://revengepornhelpline.org.uk>

Revenge porn is when someone shares a sexual video or photo of you without your consent. It's illegal for someone to do this, and there are ways to get support. If someone's threatening you or has shared an image or photo of you online, there are things you can do:

- Report it: If you're over 18 you can get support from the Revenge Porn Helpline. Take screenshots of anything you're sent as evidence.
- Don't respond to messages, comments, or threats: It can be natural to panic when you see something posted about you or someone threatens you. But don't respond to threatening messages or comments.
- Talk to someone you trust about what happened, you can get advice from the Life Lounge.

<https://www.bolton.ac.uk/student-life/student-support/life-lounge/>

<https://www.gmp.police.uk>

<https://revengepornhelpline.org.uk>

## Online Radicalisation

Part of university life is respectful debate and discussions, learning from others and valuing other people's identities, faiths and beliefs, Universities are places to help broaden minds and perspectives. This should however be within the parameters of democracy and the laws. There is no place for extremism or terrorism.

Social Media, websites and other digital channels are sometimes used to spread extreme views and ideas, this could include the promotion of hatred, violence, terrorism and non-peaceful protests. When someone seeks for you to support or share their extreme views this could be considered radicalisation. If you are approached by someone with extreme views and or feel uncomfortable about what people are saying and or sharing share your concerns.

It can be hard especially if the person sharing these views is a friend. The Home Office working with multiple organisations including the Police and Local Authorities have setup mechanisms to protect vulnerable people from be exploited by extremists, this programme is called Prevent.

Share your concerns, act early, sharing concerns may save lives. Visit ACT Early Website to find out more. In an emergency contact the Police on 999. If you want to speak with someone following sharing concerns please contact the Life Lounge.

<https://act.campaign.gov.uk>

<https://www.gmp.police.uk>

<https://www.bolton.ac.uk/student-life/student-support/life-lounge/>



## Online Shopping

Online shopping brings more risks, and more opportunity for cyber criminals to scam you out of your money or steal your personal information so it's important to make sure you're shopping safely on the web. Here are a few top tips to help you have safe and secure online shopping experience:

- Do your homework, if you're using a website you've not used before, research them online first to make sure they're legitimate, check out reviews on independent sites such as TrustPilot. Avoid clicking through to websites from pop-up ads, instead go directly to the company's website via a search engine.
- Check the website security – Look for the following signs to know whether the website is secure.
- There should be an icon of a locked padlock in the address bar next to the website address.
- The website URL should start with https:// and not just http:// - the S stands for secure.
- On some browsers and websites, the address bar will turn green to show you it is secure.
- Pay attention to any warnings about site certificates – these sites should be avoided.
- Before you go to pay, consider the security of your payment options. Using a credit card offers more financial protection than a debit card as there are more consumer protections and it doesn't give direct access to your credit. Third-party payment services such as PayPal and Google Pay are another option as you're not giving the seller your card information directly. Some banks are now also adding extra security when you're shopping online, including multi-factor authentication where you will have to pass an extra level of security to prove it's you, e.g. a one-off time-limited code sent by text.

### Looking for more information?

For more guidance and top tips on staying safe when shopping online, take a look at the National Cyber Security Centre's security advice.

<https://uk.trustpilot.com>