



SAFE ON SOCIAL TRAINING AND EDUCATION

Online Consent

www.safeonsocial.com

Online Consent

The concept of online consent has become increasingly significant, particularly in relation to social media platforms. Online consent plays a vital role in numerous aspects of social media engagement, ranging from sharing multimedia content like photographs and videos to generating user profiles and participating in online communities. It is of utmost importance for all members of the community, businesses and educational institutions to be well-versed in online consent and the accompanying responsibilities associated with social media usage.

Are people knowledgeable about their rights and obligations concerning online consent, and are they cognizant of the permissions they are granting to others? It's crucial to develop a comprehensive understanding of online consent and its application within the realm of social media.

In the same way we seek permission before divulging someone's personal information offline, online consent is crucial before sharing photos or personal details on social media. Respecting the choices of others when they withhold consent is equally important. Unauthorised sharing can lead to severe consequences, such as cyberbullying, identity theft, or legal action. Social media platforms have implemented privacy settings and consent features to help users control access to their information, but with the ever-present unauthorised content, vigilance in online conduct remains essential.

Online consent involves an individual's voluntary agreement to share their information, preferences, and content on digital platforms, as well as their willingness to be subjected to certain terms and conditions. This encompasses a wide range of activities and interactions, including subscribing to newsletters, accepting cookies, granting access to personal information, and engaging in various online transactions.

Obtaining online consent is crucial in a variety of situations. Adolescents, in particular, can be susceptible to the consequences of neglecting online consent, as they might not fully comprehend the ramifications of disseminating information on the internet. For example, if an individual intends to utilise another person's photograph or content, it is essential first to secure the owner's permission. This ensures that the material is employed respectfully and that the owner is informed about how their content will be used.

Another scenario is when someone wishes to share sensitive details about another individual. This could range from innocently sharing a friend's joyous news to more malicious attempts aimed at damaging or defaming someone's reputation. Practicing proper online etiquette involves always seeking permission from the concerned party before sharing any information online. This proactive approach can help prevent potential concerns or negative repercussions in the future.

Breaches of online consent can have severe consequences for individuals and their families, emphasising the importance of prevention.

One frequent type of online consent violation on social media is the unauthorised use of someone's photos, videos, personal information, or other content without their permission. Examples of online consent breaches encompass distributing a photo taken without the individual's awareness, uploading or circulating a recorded altercation, spreading private images, or divulging information that was shared in confidence.

To safeguard their own privacy and that of others, individuals must be cautious about what they share online, maintain positive relationships with others both on and off the internet, and monitor their digital behaviour. Families can also take measures to prevent consent breaches on their loved ones' social media accounts such as asking children for their consent before sharing their photos online. Supervising account activity, implementing parental controls, and educating family members about digital safety and consent is essential. Ensuring that privacy settings on social media accounts are appropriately configured can limit the audience and protect content from public access. Furthermore, families can encourage regular reviews of social media accounts and prompt removal of any content posted without permission.

Occasionally, people may commit errors in judgment, necessitating accountability and efforts to mitigate the aftermath. In other situations, unknown individuals may misuse someone's information or images, and there are avenues for reporting such breaches to the platform and relevant authorities.

Our top tips

1. Always ask for permission before sharing someone else's content, photos, or personal information on social media. Even ask your kids! It is the perfect way to teach them about consent.
2. Configure your privacy settings to limit the audience of your content and prevent public access.
3. Regularly review and update your privacy settings as social media platforms frequently change their policies.
4. Be cautious when accepting friend or follower requests, only granting access to people you actually know and trust.
5. Educate yourself and your family about digital safety, online consent, and responsible social media behaviour.
6. Encourage open communication within your family or community about online experiences, concerns, or incidents.
7. Report any unauthorised use of your content, personal information, or breaches of consent to the social media platform and relevant authorities.
8. Be mindful of the potential consequences of sharing content online, including the possibility of it being misused or taken out of context.
9. Set up parental controls on devices used by minors to monitor and restrict their online activities.
10. Refrain from engaging in cyberbullying or spreading rumours, as these actions can cause harm and may lead to legal consequences.
11. Be respectful of other people's choices and decisions, especially when they decide not to give their consent for content sharing.
12. Be mindful of the risks associated with sharing location data, as this can compromise personal safety and security.

13. Limit the amount of personal information you share on your social media profiles, such as your or your family members address, phone number, or birthdate. Think twice before sharing photos of birthday cakes and their age!
14. Use strong and unique passwords for each of your social media accounts and enable two-factor authentication when available.
15. Be cautious when clicking on links, even from trusted sources, as they may lead to phishing sites or contain malware.

In cases of online consent breaches or other cyber incidents, you can report them to the appropriate authorities in each country. Here's where to report in Australia, New Zealand, Hong Kong, and the UK:

Australia: You can report cyber incidents to the Australian Cyber Security Centre (ACSC) through their ReportCyber tool, available at <https://www.cyber.gov.au/acsc/report>. For issues related to online safety, harassment, or cyberbullying, the eSafety Commissioner is the responsible authority, and you can find their reporting tool at <https://www.esafety.gov.au/report>.

New Zealand: In New Zealand, you can report cyber incidents to the government agency CERT NZ (Computer Emergency Response Team) by visiting <https://www.cert.govt.nz/individuals/report-an-issue/>. For online safety and cyberbullying concerns, you can reach out to Netsafe at <https://www.netsafe.org.nz/report/>.

Hong Kong: For cyber incidents in Hong Kong, you can report to the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) via their website at https://www.hkcert.org/report_incident. Additionally, the Office of the Privacy Commissioner for Personal Data (PCPD) handles personal data privacy issues, and you can file a complaint at https://www.pcpd.org.hk/english/complaints/how_to_file_a_complaint.html.

United Kingdom: In the UK, you can report cyber incidents to the National Cyber Security Centre (NCSC) by visiting <https://www.ncsc.gov.uk/report>. For online safety and cyberbullying concerns, you can visit the UK Safer Internet Centre, which provides resources and reporting options at <https://www.saferinternet.org.uk/>.

Please note that in most cases, you should also report any breaches of online consent or cyber incidents to the respective social media platform first, as they have their own reporting systems and mechanisms to handle such situations and authorities usually ask if you have reported to the platform so take a screenshot for your records.

www.safeonsocial.com

No part of this e-book/cheat sheet or its associated modules may be reproduced or transmitted by any person or entity in any form or by any means, electronic or otherwise including photocopying, recording or scanning or by any information storage without prior permission from Safe on Social Media Pty Ltd other than the licensor who is licensed to use this information in newsletters and in print and has been granted permission from the publisher under an annual license.

The publisher, authors, licensee, licensor and their respective employees or agents will not accept responsibility for injuries or damage, physical or emotional occasioned to any person as a result of a social media use or any other activities described in this e-book/cheat sheet, very attempt has been made to ensure that the information in this e-book/cheat sheet is accurate,

it is the nature of social media to be constantly changing.

Therefore, Safe on Social Media Pty Ltd gives no guarantees and accepts no responsibility to the completeness or accuracy of the contents of this guide.