



## BROMSGROVE SCHOOL

# STAYING SAFE ONLINE

### PROTECTING YOURSELF

- When you are online think about the four areas of potential risk:




**Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

**Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

**Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying,

**Commerce:** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group <https://apwg.org/>

- Always think before you send or share as the content may become public and permanent. Comments, actions, or images can stay online even if they have been deleted. You do not know who else has downloaded the image or what search engine identified and cached your photo.
- There will be times when you enter your personal information online, for example, when you make an online purchase and register for a recognised website. Always ensure that the webpage is encrypted (address starts with https and shows a padlock symbol  in the address bar).
- On social media other similar websites, be careful in what personal information you disclose about yourself or others (this could include addresses, email addresses, telephone numbers, age and birthday). Never disclose your full date of birth, car registration or bank details, including memorable security information. This information is integral to your security and could leave you at risk of privacy breaches or identity fraud. Sharing the wrong sort of information, posts and pictures could also have an impact on your employability and employment.

- If you like using geotagging and tagging, then it is better to do it retrospectively, after the event. Giving away your current location has risks. As an adult, stating that you are away from home or posting holiday pictures can invalidate insurance policies and can make your home vulnerable.
- Use the privacy and security settings on social media sites so that only friends and family can see your pages. You can alter settings to control who can see your posts, who can contact you, who can tag you and what types of adverts are displayed on your feed. You can create 'friend lists' to share information with a specific audience. You can disable and change app settings and block app requests.

If you've stopped using a social media site or forum, suspend the account and wipe the content.

- Be aware of spam, phishing and viruses. If you receive emails from companies and websites requiring information, go to your account directly rather than clicking on email links.
- Make sure you have a firewall and full, active versions of anti-virus software and anti-spyware on your computer. Also be careful what you download or install on your computer, particularly browser extensions as they can show your data and browsing habits and may even be malicious.

A firewall will stop unauthorised people hacking on to your computer, anti-virus programmes will guard your computer from viruses which could destroy your computer and anti-spyware will look out for programmes which spy on your computer use in an attempt to learn passwords or account details.

## PASSWORDS AND SECURITY QUESTIONS

- Never share or reveal your passwords. Try to use strong passwords that are hard for others to guess. They should be at least eight characters long using a mix of lowercase and uppercase letters, at least two numbers or symbols and not contain any complete words.
- Use unique passwords for websites where security is extra important, like banking websites. For other websites, use different passwords - to make it easier to remember, you can use different variations of the same password.
- Change your password regularly. If you find it difficult to remember your passwords, write down a hint rather than your entire password.
- Never share or reveal answers to security questions, such as, your mother's maiden name, your first pet/car/concert/road/school.

## CYBERBULLYING AND CYBERSTALKING

- The best way to deal with cyberbullying is to 'stop, block and tell'. STOP communication by not answering back, as that will only feed the abuse, BLOCK the person or message and TELL

someone. At School there are many people you can tell :Houseparent, tutor, teachers, they will be able help you. Understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it's never too late to tell someone.

- When communicating with others, be polite and responsible. Do own everything you say and speak only for yourself. Be the same friend online as you are in person and think about the effect your post will have on other people. Do report if you see any of your friends being bullied.

## FORMS

- When you're signing up for an account, make sure you look for the box near the bottom, which asks if you want to receive more information. Some require you to tick them to opt-in, some require you to tick them to opt-out, so read it carefully. Only fill in the mandatory boxes, marked with an asterisk \*. Some companies will sell your personal data, so make sure you take time to tick/untick the right boxes.

## REPORTING, SETTINGS AND ADVICE

- Reporting at School: [online@bromsgrove-school.co.uk](mailto:online@bromsgrove-school.co.uk)
- CEOP <https://www.ceop.police.uk/ceop-reporting/>
- UK Safer internet centre <https://saferinternet.org.uk/>
- Childline <https://www.childline.org.uk/>
  
- Anti-Phishing Working Group <https://apwg.org/>
- Snapchat: <https://www.snapchat.com/privacy>
- TikTok. <https://support.tiktok.com/en/safety-hc/report-a-problem>
- Discord <https://support.discord.com/hc/en-us/articles/360000291932-How-to-Properly-Report-Issues-to-Trust-Safety>
  
- Instagram: <https://help.instagram.com/>
- Twitter: <https://twitter.com/support>
- Facebook: <https://www.facebook.com/help/>
- Think U Know: [https://www.thinkuknow.co.uk/14\\_plus/](https://www.thinkuknow.co.uk/14_plus/)
- Childnet: <http://www.childnet.com/young-people/secondary>