Internet Safety

Social Media Best Practices

- **Private accounts.** It is best practiced to keep your social media accounts on private. Instagram, Facebook, TikTok, and Twitter all have features to limit who has access to see your content. This will be added protection for sensitive information. But even a private account is not completely safe. It is always good to be cautious of what you post. Even if your account is private, it is not completely safe. Do not post anything you would not be comfortable with everyone seeing. Do not post drug or alcohol references, as these are
- **Your reputation matters.** Even when you have a private account, your information is not completely safe online. People who you don't think will see your account might see what you post. Potential employers, supervisors, and teachers might browse social media and come across your page. This is a large issue on TikTok, which syncs the contacts in your phone to promote your videos onto your contact's 'For You Page'. If you have a supervisor's number, your TikTok videos might come up on their feed. Always ask yourself how your posts might be interpreted by others.
- Anything online can be altered, faked, and sent around. Once something is online, it can be taken out of context to harm others. This includes hurtful messages and photos of sex, drugs, and alcohol. If you do not feel comfortable pasting something on the walls of IES Delgado Blackenbury, do not post it online!
- **Avoid 'spilling tea'.** Do not forward or share harmful or embarrassing photos, even of your friends. You don't know how someone might react. Also, do not impersonate anyone on social media.
- **Don't post your location.** Do not constantly post your location, as this very dangerous. Turn 'SnapMaps' on Snapchat off! You do not need to give everyone access to your whereabouts at all times; this can make you susceptible to predators.
- **Touch grass.** It is easy to spend hours and hours on social media. It can be a real time-suck. Make sure you do other things, like finishing homework, practicing physical activity, listening to music, or reading.

Online Safety

When online, never allow other people to access this information.

- your full name
- your current location
- home or school address or the address of any of your family or friends
- phone numbers
- NIF number
- passwords
- names of family members
- credit card numbers

Protecting your wallet.

- Looking at the address bar of the website you are using. An s in "https://"' means there has been some security incorporated into the website. A lock symbol signals that there is a secured encryption processes to transfer data and protect you from hackers.
- Legitimate website usually have a contact page and a social media presence. If something looks fishy or too good to be true, it likely is. Do not give out your credit card or personal information to websites that do not seem trustworthy. It also is good practice to search up the website and read reviews from other sources.

**IES
Delgado
Brackenbury**

Made by Joseph Kazancioglu