Digital Safeguarding – Online Safety Information for Parents and Students

At Tiffin Girls' School, we are committed to supporting our students to be safer online. We believe that technology can be a force for good, but it is crucial for families and the school to work together through dialogue to ensure it is used safely. We have compiled important information and tips to help you support your child's online safety.

Key Areas and Tips for Parents:

1. Understanding Device Use

Devices have changed significantly and effectively all perform similar functions now. While families may treat devices differently, children can use all their devices interchangeably. Apps on a mobile phone often work on laptops, Chromebooks, and sometimes smart TVs.

- Ask yourself: Do you know *how* your children use all of their devices?
- Do you know *where* they use them?
- Do you know *when* they use them?
- What family protocols are in place to ensure all devices are used as safely as possible?
- Consider keeping phones and laptops out of bedrooms.
- Monitor your child's wider use of technology.
- Do you know the webpages they are using?
- Do you know which gaming platforms they are using?
- Do you know the contacts/friends that they have online?

2. Parental Controls and Device Settings

Staying on top of parental controls is vital across all devices used by your family at home. Regularly check the controls on all your devices.

- Start by checking your broadband and Wi-Fi settings.
- Use filters and set them up on all devices connected to your home broadband.
- Also, check filters available on other apps and online services your family uses regularly, such as TV channels.
- You have the ability to look at content filters, chat filters, privacy settings, and control any purchases your children may make.
- Ensure you have parental controls set up on your child's devices.

<u>On iPhone:</u> Settings > Screen Time > Content & Privacy Restrictions

Restrict explicit content, websites and in-app purchases

<u>On Android:</u> Use Family Link to approve downloads and block websites.
In the Google Play Store: Settings > Parental Controls

3. Managing Device Usage and Time Limits

It is possible to set limitations on how devices are used. Reports indicate that the average child in the UK spends over two hours a day just on TikTok alone.

- Look at the parental controls on your child's mobile phone and all other devices they use.
- You can control and limit the amount of time children use devices, both overall and for individual apps throughout the day.
- This control can often be managed through your own devices.
- A quick tip is to spend a short amount of time (30 seconds to a minute) checking that your device and app settings are configured as you wish.
- Have a dialogue with your child about *what, when*, and *how* they access information through their mobile phone and other devices.
- Have time limits set up for device usage.

On iPhone: Settings > screen time > app limits - you can also set downtime for device free time

On Android: Use Digital Wellbeing > Dashboard to view and limit screen time.

Or use **Family Link** to pause apps and set daily limits.

4. Contacts and Online Friends

Children often feel significant pressure to accept many online contacts, sometimes numbering in the hundreds. It's important to have a dialogue with your child about their online contacts.

- Discuss with your child if they actually know who their contacts are and how they know them.
- Ask yourself as a parent if you understand who these contacts are and if you know them in person.
- Students have been encouraged to review their "friends" across social media platforms, removing those they no longer want or are not in contact with. More importantly, they should review who their "friends" are and remove anyone they don't actually know.
- Consider if you know all of your child's online 'friends' or followers.

5. Online Reputation and Digital Footprint

We have discussed with students the importance of thinking about their online reputation or digital footprint.

- Things typed or posted online now can have serious implications for them now, in the medium term, or long term in the future.
- Online posts may have serious implications for college, university, or future job applications, as employers, colleges, and universities may look online for more information.

6. Age Appropriateness of Social Media and Apps

Most social media platforms have an age limit of 13 plus. While children may feel pressure to join before 13, this does not mean they should. Even if a child is 13 or older, it doesn't automatically mean they should join.

- The important thing is for your family to make decisions together and allow your child to join when you, as the parent, feel comfortable.
- It may be beneficial to sit down together, check out the site or app, and work through its key components and how to use it.
- Discuss how the use of the app will be supervised. Some families choose to follow their children online, while others agree on times to sit together and review social media posts and contacts.
- Ensure you know if the apps being used are age appropriate.

Other Important Online Safety Topics:

Students have also engaged in assemblies covering key online safety topics, including:

- Misinformation & Fake News: How to know what to trust. This includes using reliable sources and cross-checking information. Quick tips include fact-checking, thinking before sharing, and being sceptical of clickbait. We discussed examples like AI-generated images, fake news headlines, and misleading statistics.
- Privacy & Data Protection: Are you in control of your personal information? Students were advised to review and update social media privacy settings.
- AI & Deepfakes: Can you spot what's real and what's artificially generated? We are thinking deeply about the impact AI will have on children and the need to educate and protect them.
- Cyberbullying & Online Harassment: How can we create a kinder digital space? Being a digital role model, promoting positivity, and challenging harmful content is important.
- Screen Time & Wellbeing: Are you managing your online and offline balance? Taking breaks and balancing screen time with offline activities is encouraged.
- Protecting Accounts: Use Two-Factor Authentication to protect accounts from hacking.

School Policies and Reporting Concerns:

- Students sign and agree to an Acceptable Use Policy each year which allows them to access the school digital systems.
- There are a range of policies that support the safe use of technology. This includes:
    - E-Safety
    - Data Protection
    - Privacy Notice – Students/staff
    - Artificial Intelligence
    - Anti-Bullying
    - Behaviour for learning
    - Online Safety
    - Safeguarding
- Chromebooks are available for student use, and we monitor student technology use on and offsite through Senso and filtering is provided by the London Grid for Learning.

- Mobile phones can come into school but must be away and turned off unless there is explicit permission from a member of staff.
- Students are not to take or use images of staff.
- Students have been reminded how they can report any concerns they have to us at the school by emailing the dsl team or by contacting any member of staff. Students can also use the Anonymous Reporting Form. Or online through the "CEOP button" available on the school website.

If you, as a parent, have any concerns about the safety of a child at The Tiffin Girls' School, please get in touch with us. Our dedicated safeguarding team email address is **dsl@tiffing.org**

Published: May 2025