CCSD Administrative Guidelines Regarding Internet Safety

Pursuant to the School Board's Internet Safety Policy (IFABB), these administrative guidelines are to be utilized by CCSD staff in policy application::

1. Do not post personal information on websites, chat room profiles, text messaging profiles or in emails. Personal information includes your legal name, last name, home address, phone numbers, relationship status, date of birth, gender, financial information, insurance information, social security number, passwords, logon information and other usernames.

2. A basic strategy to avoid identity theft and online fraud is to keep your personal information private when you go online. Be equally careful about sharing information offline and be sure you know how organizations will use your information before you give it to them.

3. Choose a screen name that does not identify you.

4. Do not share your passwords with anyone.

5. Use "strong" passwords that you can remember and do not write them down where they can be seen or taken. The strength of a password is a function of length, complexity, and unpredictability. A strong password generally is greater than eight characters in length and contains at least one uppercase letter, one number, and one symbol (i.e. Pa$sW0rd).

6. If the service allows, make up your own password reminder questions. Choose this option instead of using pre-defined security questions.

7. Do not respond to any emails or text messages requesting personal information.

8. Do not open emails from unknown senders.

9. Use caution in trusting a message that appears to be from someone you know. Hackers can break into accounts and send messages that look like they're from your friends/colleagues. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out. This includes invitations to join social networks.

10. Assume that everything you put in any electronic format is permanent. Even if you delete the content or your account, anyone on the Internet can easily save, print or forward photos, text or videos to a computer or the information may be cached on another server.

11. Before you post or send content, assume everyone can see what you post. Anything sent in a text, including sexually explicit or provocative images, can be easily forwarded and made public.

12. Respect others' privacy. Posting an embarrassing photo or forwarding private text without asking can cause unintended hurt or damage to others.

13. Use privacy settings. Most social networking and photo-sharing sites allow you to determine who can access and respond to your content.

14. If you find information about yourself online that is unappealing, embarrassing, or untrue, contact the website owner or administrator and ask them to remove it or look for an option to report violations. Most sites have policies to deal with such requests.

15. Tell a trusted adult if anything happens online or if you receive a text message that bothers or frightens you.

16. Do not arrange to meet anyone you have met on the Internet without telling a trusted adult.

CCSD Administrative Guidelines Regarding Internet Safety

Pursuant to the School Board's Internet Safety Policy (IFABB), these administrative guidelines are to be utilized by CCSD staff in policy application::

17. When conducting a video conference, do not accept invitations from unknown users that request to be added to your contacts.

18. Do not accept files that are suspect or from unknown users while participating in a video conference.

19. Keep in mind that many video conferencing solutions allow for recording. Do not say or do anything in the conference that you would want to be made public.

20. Illegal downloading, digital cheating and copying other people's content may be easy, but that does not make it right. You have the responsibility to respect other people's creative work -- and the right to have your own work respected.

21. Create, share, tag, comment and contribute to the online world in positive ways.

22. Mobile devices should be protected to guard against identity theft. This is especially true if the mobile device has applications ("apps") with access to social networking or other sites containing personal information.

23. Mobile devices are not immune to viruses and malicious code. Use caution when downloading files or browsing websites.