Classroom Discussions About Computer Safety and Digital Citizenship

Rationale: Students have more exposure to digital technology and the Internet today than ever before. Whether it is accessing the Internet from an iPod, an iPhone, or from a laptop, students need to be taught how to protect themselves and their computing devices when on the Internet. Teaching students about the concepts outlined below is necessary due to the recent proliferation of parent-supplied mobile devices used by students at school and due to the increasing use of school-provided computers for everyday classroom learning. Developing an understanding of these concepts will help students to protect themselves from identity theft and help them to become good digital citizens.

General Computer Terminology discussions include (as appropriate):

- What is a computer (display, storage, CPU, WiFi, USB, sensors).
- What is an operating system (Linux / Mac / Windows / Android / iOS)
- What is the ‘cloud’ versus a network drive or a hard drive.
- Differences between Google Docs and OpenOffice / LibreOffice
- What is wireless networking (WiFi, Bluetooth, Near Field Communications(NFC)).
- What is the Internet (routers / servers / activity logs).
- What is an IP (Internet Protocol) Address and how does it identify a device.
- What is network bandwidth and how is it shared by devices.

General Computer Safety discussions include (appropriate to grade):

- Protecting your personal information (never share your name, photo, address, phone number, password, family plans).
- How to deal with accidental discovery of inappropriate Internet material.
- Appropriate use of pseudonyms if required to access online services.
- Ethical considerations about logging into someone else’s account.
- Understanding security vulnerabilities in Internet of Things devices (web cameras).
- How to create a secure password.
- How to understand the difference between safe and unsafe email attachments.
- How to recognize phishing emails that attempt to steal account information.
- How to recognize Javascript browser hijacks & lockups with phony security warnings.
- How to detect fake application upgrade prompts in a web browser.
- Limitations of Tor networking and the Dark Web.
- Importance of keeping software updated.

- Understanding how network administrators can track computer usage.

Mobile Device Safety discussions include (appropriate to grade):

- How phones / tablets can leak information about you through malicious apps.
- Ability of any software on your phone to surreptitiously take your picture.
- How to protect information on your personal device (phone / tablet).
- Limitations of current biometric authentication technologies.
- Limitations of encryption apps (Telegram / Whatsapp).
- Dangers of connecting to public WiFi hotspots (man-in-the-middle attacks).
    - Plaintext transmission of sensitive passwords.
    - Importance of using https to encrypt data.
    - Tendency of public routers to take your picture (Meraki routers).
- Dangers of renaming your device (ie: Jeff's Phone).
- Dangers of leaving Near Field Communication and Bluetooth radios activated.

Digital Citizenship discussions include (appropriate to grade):

- Persistence of online information (messages / pictures / comments / YouTube videos).
    - Legal warrants for access to information saved on a server.
    - Employer screening based on online information (thinking about your future).
- Laws against distribution of underage nude photos (sexting).
- Copyright laws and considerations for sharing digital texts.
    - Restrictive copyright versus permissive copyright.
- Cyberbullying:
    - Ethical and legal concerns over cyber vigilantism ('creep snatchers').
    - Dos and Don'ts when commenting on someone else's work.
- Ethical considerations for events broadcast or viewed on live streams.
    - Your responsibility to report preventable live-stream crimes / suicide.
- Limitations of anonymity on the Internet.
    - Legal proscriptions against impersonating another person (identity theft).
    - Limitations of pseudonyms in protecting your identity (IP tracking).
- Danger of arranging with people online to meet in person.
- Hacking groups (Anonymous) and social engineering (phishing).

Environmental Considerations of computer technology (social responsibility):

- Benefits of a paperless classroom.
- Responsible printing practices.
- How to dispose of obsolete electronic devices.