# IIBG Computer and Device Use

Use of District Computers and Devices/Privacy Rights

District-issued computer systems and electronic devices (including, but not limited to, Interactive displays, iPads, iPhones, Chromebooks, eReaders, and eBooks) are for educational and professional use only. All information created by staff and/or students or stored thereon shall be considered district property and shall be subject to unannounced monitoring by district administrators. Unauthorized access to and/or unauthorized use of the district server or security system (including, but not limited to, surveillance footage) is also prohibited. The district retains the right to discipline any student, up to and including expulsion, and any employee, up to and including termination, for violation of this policy.

Copyright

Software acquired by staff, using either district or personal funds, and installed on district computers or electronic devices must comply with copyright laws. Proof of purchase (copy or original) for software must be filed in the technology department.

Installation

No software, including freeware and shareware, or other applications may be installed on any district computer or electronic device until cleared by the network administrator. The administrator will verify the compatibility of the software or application with existing software, hardware, and applications and prescribe installation and de-installation procedures. Program files must have the Technology Director's approval to be installed on any district server or computer. For Chrome devices, users are allowed to install any app listed on the Santa Fe Trail Chrome Web Store without prior approval.

Hardware

Staff and/or Students shall not install unapproved hardware on district computers or make changes to software settings that support district hardware.

Hardware Care & Maintenance

Proper care for any device involves a combination of physical maintenance, software management, and general handling practices. Here's a detailed guide:

- Keep it Clean: Regularly wipe the screen, keyboard, and exterior of your device with a soft, dry cloth to remove dust, fingerprints, and other debris. Avoid using harsh chemicals or abrasive materials that could damage the surface.
- Handle with Care: Treat your device gently, avoiding dropping or mishandling it. When transporting it, use a protective case or sleeve to shield it from scratches and impacts.
- Power Management: Power down your device properly when not in use instead of just closing the lid or just leaving the screen on. This ensures that updates are installed and conserves battery life.
- Software Updates: Allow your device to install software updates regularly. These updates include security patches, bug fixes, and performance improvements. Modern devices typically update automatically when connected to the internet.

- App Management: Install apps only from the official App store, Chrome Web Store or Google Play Store. Avoid downloading apps from untrusted sources, as they may contain malware or other security risks.
- Storage Management: Most devices have the ability to store data on cloud storage, but if you store files locally, periodically clean out unnecessary files and apps to free up space and maintain performance.
- Security Awareness: Be cautious when browsing the web and downloading files. Avoid clicking on suspicious links or downloading attachments from unknown sources to prevent malware infections.
- Temperature and Environment: Keep your device in a temperate environment away from extreme heat or cold. High humidity can also be damaging, so avoid exposing it to moisture.
- Battery Care: Avoid consistently draining the battery to zero. Instead, aim to keep it between 20% and 80% charged for optimal battery health. If storing for an extended period, charge the battery to around 50% before storing it.
- Peripheral Use: Be cautious when using accessories such as chargers, mice, or USB drives to prevent damage to ports or other components.

Audits

The administration may conduct periodic audits of software and applications installed on district equipment to verify legitimate use.

Email Privacy Rights

Employees and/or students shall have no expectation of privacy when using district e-mail or other official communication systems. Any email or computer application or information in district computers, computer systems, or electronic devices is subject to monitoring by the administration.

Ownership of Employee Computer and Device Materials

Computer materials, devices, software, or applications created as part of any assigned district responsibility or classroom activity undertaken during school time shall be the property of the board.

Lost, Stolen, or Damaged Computers and/or Equipment

Students and staff must reimburse the district for the replacement or repair of district-issued computers or electronic devices if they are lost, stolen, or damaged while in their possession. However, the Superintendent may choose to waive this fee in cases of theft upon presentation of a police report.

Fees / Replacement Cost

- There will be a $40 repair fee for:
    - Minor damages to the device requiring replacement parts or repair
    - Damage or loss of the charger
    - Damage or loss of the case
- A $300 replacement fee will apply for Chromebooks, with costs for other device types to be determined, for:
    - Intentional damage making the device reasonably non-repairable
    - Loss of the device
    - Excessive damage
- Subject to the building administrator's discretion and device availability, we will provide a substitute device for use while your original device is being serviced.