Instructional Programs

3. Technology

During the COVID-19 pandemic, technologies are playing a crucial role in keeping our schools functional in a time of lockdowns and quarantines. These technologies may have a long-lasting impact beyond COVID-19.

- Continue to monitor the technology hotline to serve as a support to students, parents, and staff
- Equip technology devices with the necessary software for students to submit class assignments
- Review campus inventory and identify the number of devices needed to ensure 1 device to each student
- Serve as resource to campus staff to support remote instruction
- Provide guidance to campus technology support technicians (TST) to support parents with technology and software program needs.
- Identify potential trainings needed and collaborate with staff in the professional development office to provide professional development

Instructional Programs continued Technology

- Provide support to staff to understand student data privacy and technology issues in the cloud.
- Collaborate with Special Services to support equitable technology access to students with special needs
- Create an awareness of data privacy laws and policies and the severity of data disclosure
- Verify that technology structures are in place for trusted learning environments and secure student data
- Protect technology resources by mitigating risks and creating a district wide and community security awareness for a secured BISD Trusted Learning Environment

Instructional Programs continued Technology

The technology team will:

- Provide a **list approved cloud application**
- **Educate** district's staff, students and parents on **common cybersecurity, best practices, and red flags.**
- **Monitor account logins** and anomalous behavior (account takeovers)
- Properly **vet 3rd party apps.**
- **Look at external accounts and if shared** break them and set policies to remediate future external sharing.
- **Delete emails** that contain files, with security numbers, W2's, and bank account information.
- **Monitor signals** of cyberbullying, self-harm, inappropriate content, abuse, and other safety threats.
- **Ensure district devices have anti-phishing and anti-malware protection.**
- **Establish a multi-factor authentication-a second step**, after entering the correct password to prove they authorized.
- **Reset and strengthen passwords**- maximum password lengths, password expiration, and more.
- **Run a cloud security audit to check** configuration errors, sharing risks, files information to 3rd parties, and more.