THE DOWNLOAD

INFORMATION TECHNOLOGY UPDATES FOR EHSD STAFF

What Your IT Team is Working On

Upgrading to Windows 10, version 20H2

Some new features are:

› A simplified way to make changes, improving IT's ability to quickly address equipment issues

› A better visual experience with a user interface that has a more consistent look between the start menu and icons

› Enhanced security features focusing on the ever-evolving waves of cyber attacks

Keeping Track of Equipment: We are finalizing the IT equipment inventory. If you have not had IT inventory your on-premise or portable equipment, call the Help Desk (925) 521-7200 to set up an appointment for a technician to check the equipment. Portable equipment includes items like iPhones, iPads, laptops and projectors. For bulky items such as monitors and mini PCs used for remote work, photos of their asset tags are sufficient. Be sure to check any drawers and cabinets for equipment, as we must include all items in the inventory.

IT is "In the Know": You can be confident that you are using the most up-to-date software at EHSD. Your IT Team regularly reviews vendor announcements to ensure that we are on the latest version. In addition, we scan industry announcements to keep track of potential changes headed our way.

Testing, Testing

Azure Virtual Desktop (AVD) Deployment: IT has completed testing for AVD. Thanks to all who participated, including the Head Start team whose real-world fire damage provided the opportunity to see how fast and how robust the environment can be. IT plans to move forward with the rollout of AVD soon, and we will have more details for you as we get closer.

Cybersecurity

iPhone Multifactor Authentication: Verifying ID to use a county iPhone for email access is important for cybersecurity. Contra Costa County required the enabling of multi-factor authentication (MFA) on computers and laptops used outside of EHSD buildings in order to enhance our email security. This now includes iPhones and iPads, and you can use the same account in Microsoft Authenticator for confirming identity when using these devices.

MFA requires you to present two pieces of evidence to an authentication mechanism such as a password and a one-time code or push notification. MFA dramatically reduces the risk of successful phishing and malware infections. Even if an attacker gets your password, login in not possible without a second piece of evidence.

Ask IT
What topics would you like to hear about from IT?
Email **kgaughen@ehsd.cccounty.us**.