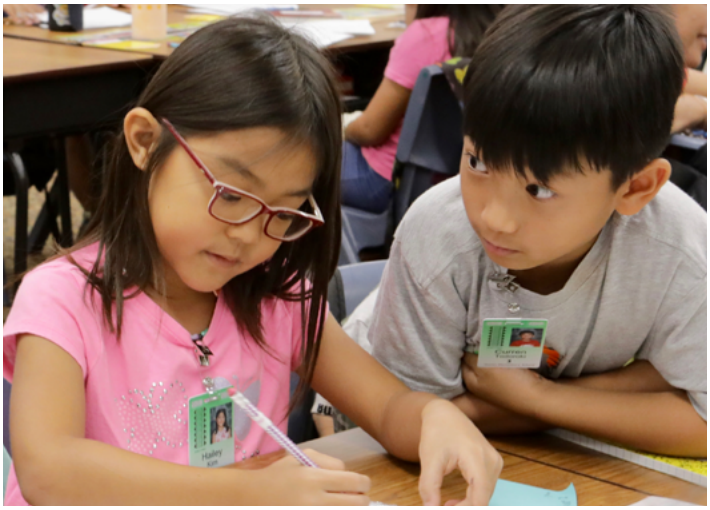
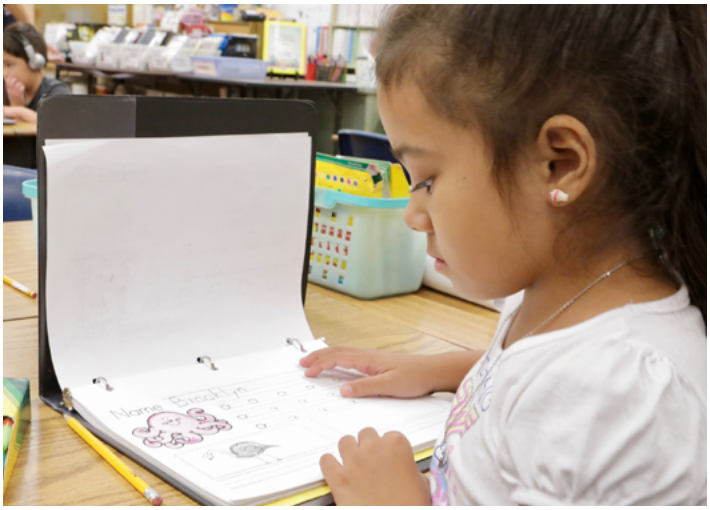
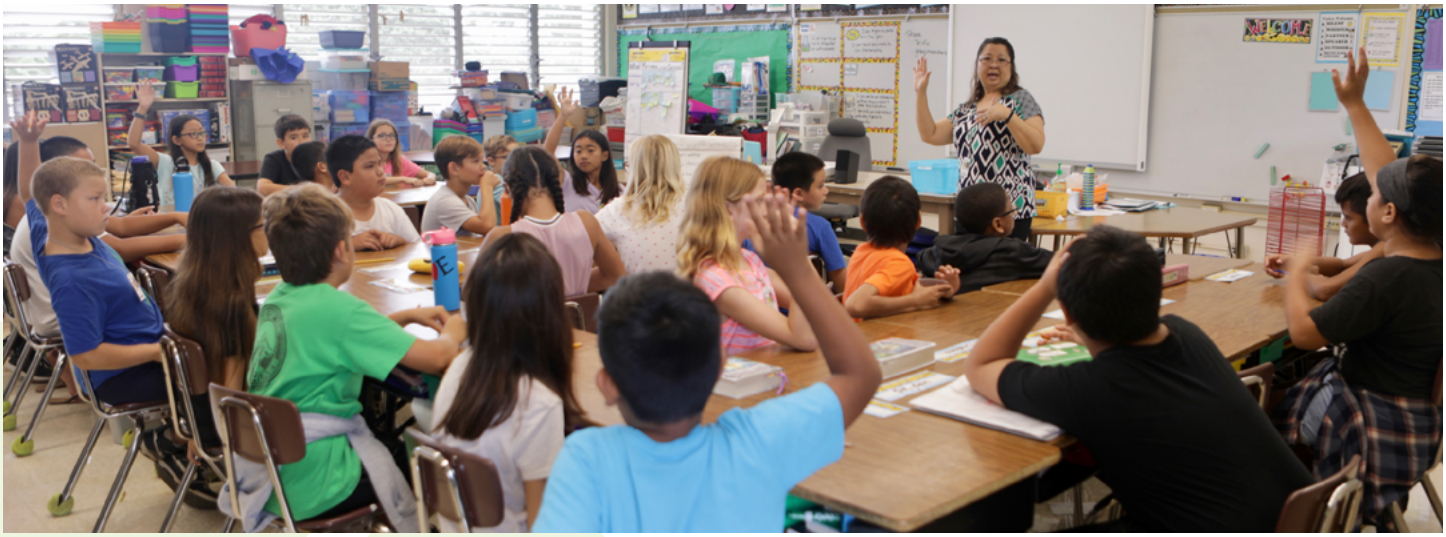
# HIDOE Technology Guidance for Employees







HAWAIʻI STATE DEPARTMENT OF EDUCATION

April 2020

**TABLE OF CONTENTS**

**TABLE OF CONTENTS (continued)**

## A NOTE ABOUT THIS TECHNOLOGY GUIDANCE DOCUMENT *As of 4/15/20*

During this unpredictable and ever-changing COVID-19 pandemic period, work and learning environments have had to adjust to traditional on-site "brick and mortar" processes to remote and virtual ones.

This document provides information, guidance, and best practices related to technology to enable HIDOE to continue with its work, teaching, and learning as much as possible. As with the ever-changing situation, this document is also meant to be a "living", ever-changing document that will be updated as decisions are made, processes are adjusted, and new information is provided.

This document combines new information and guidance with ones that were previously published under the document title *Technology Guidance & Resources During Emergency Situations.* The earlier document was posted to ServiceNow and will be replaced with this one.

## Introduction

Digital citizenship is about much more than online safety. It is a concept that helps teachers, parents, students, technology leaders, etc. understand what technology users should know to use technology appropriately. It is about behavior, ethics, respectfulness, responsibility, safety – all the things that help a technology user build and shape a digital footprint that is positive and effective.

## Characteristics of a Good Digital Citizen

- A good digital citizen is…
  - careful about what is shared online
  - treats others well by providing positive comments, telling the truth, and being polite
  - safe and doesn't divulge personal information, passwords, addresses, etc. to strangers
  - aware of the rules and terms of use of online sites, applications, social media, etc.
  - vigilant and looks out for bad behavior like cyberbullying, unwanted solicitations, etc.
  - respectful and doesn't share content that they don't own or is copyrighted without getting permission and giving credit to the source
  - aware that not everything online is true and searches for facts
  - aware that once something is posted online, it is there forever
  - careful about managing the amount of time spent online
  - aware of and follows acceptable use guidelines, policies, etc. that are set by their employer or school and does not misuse technology and resources

## Digital Citizenship Resources

| | |
|---|---|
| International Society for Technology in Education (ISTE) | Digital citizenship website provides posters, videos, books, etc. for teachers: https://www.iste.org/learn/digital-citizenship |
| | 9 resources for teaching digital citizenship provides infographics, free lessons, etc. for teachers: https://www.iste.org/explore/digital-citizenship/9-resources-teaching-digital-citizenship |
| | Digital citizenship standards for students: https://www.iste.org/standards/for-students |
| | Digital citizenship standards for education leaders: https://www.iste.org/standards/for-education-leaders |
| Commonsense.org | Essential digital citizenship lessons for the Coronavirus pandemic – provides resources for online communication, social media, and cyberbullying, resources to share with families, etc.: https://www.commonsense.org/education/coronavirus-resources |

| | |
|---|---|
| | K-12 digital citizenship curriculum with lesson plans, videos, student activities, assessments, professional learning tools, and family outreach tools: https://www.commonsense.org/education/scope-and-sequence |
| HIDOE Resources | Digital citizenship flyer provides information on appropriate media use and internet safety: https://docs.google.com/presentation/d/1qWGz4boHFXHKd7Fx90rQDWBb25KUZemNZ_Nek1zlhzM/edit#slide=id.p |
| | Child internet safety resources flyer provides information and tips from the Hawaii Attorney General's Office and information on how to enable safety features and parental controls on computers: http://www.hawaiipublicschools.org/DOE%20Forms/Emergencies/OITS%20Child%20Internet%20Safety%20Resources.pdf |
| | Continuity of Education website for students and parents provides information on acceptable media use, "Netiquette" for students, responsible use guidelines and information for parents: https://sites.google.com/k12.hi.us/resources-student-parent/parents-caregivers |
| | Computer science standards website provides information on the types of information students should learn about as part of a computer science curriculum, including standards/expectations for online behavior: https://www.csteachers.org/Page/standards |

## ELECTRONIC CONFERENCING (E-CONFERENCING) *As of 4/20/20*

**Introduction**

E-Conferencing is a method to conduct meetings, conversations, interactions, etc. in a virtual setting. E-conferencing enables users to conduct real-time collaboration, screen sharing, document sharing, and online meetings. These virtual sessions can be a one-way content sharing of information such as a web conference or webinar, or it can be a full, real-time audio and/or video communication session such as a video conference.

There are a wide variety of free and paid e-conferencing applications on the market. The Hawaii Department of Education has currently acquired three applications that are centrally managed and supported: Webex, Google Hangouts Meet (via Google's G Suite for Education), and Blackboard.

**HIDOE Centrally-Managed E-Conferencing Applications**

There are a wide variety of free and paid e-conferencing applications on the market. The Hawaii Department of Education has currently acquired three applications that are centrally managed and supported: Webex, Google Meet (via Google's G Suite for Education), and Blackboard. In addition, HIDOE is currently working to acquire Zoom.

| Product/Application | HIDOE Use | Notables |
|---|---|---|
| **Webex**<br>*Video conferencing; online collaboration* | Centrally acquired; managed by the Office of Information Technology Services (OITS) | ▪ HIDOE accounts accommodate up to 1,000 participants in one session.<br>▪ Centrally-managed version was vetted by HIDOE for security and privacy compliance |
| **Google Meet**<br>*Video conferencing* | HIDOE enterprise tenant (@k12.hi.us) centrally acquired; managed by OITS; some schools also manage their own tenants | ▪ Google has temporarily made available enhanced features in Meet through September 30, 2020. HIDOE has enabled these features in its enterprise tenant. Advanced features include:<br>▫ Sessions for up to 250 participants<br>▫ Live streaming for up to 100,000 viewers within tenant<br>▫ Ability to record meetings to Google Drive<br>▪ Centrally-managed tenant was vetted for by HIDOE security and privacy compliance |

| | | |
|---|---|---|
| Blackboard<br>*Web conferencing; learning management* | Centrally acquired; managed by the Office of Curriculum and Instructional Design (OCID) | ▫ Centrally-managed version was vetted by HIDOE for security and privacy compliance |

**E-Conferencing Applications not Centrally Managed by HIDOE**

HIDOE staff have raised questions about using e-conferencing and online meeting applications that have not been vetted by and/or are not centrally managed by HIDOE. While many of these applications can be FERPA compliant, they are only compliant when a school, complex area, or state office has entered into a proper contractual agreement (e.g., legal contract, data sharing agreement, etc.). For individual schools that have a contractual agreement with an e-conferencing vendor, they may move forward with using the application. HIDOE continues to strongly recommend using centrally-managed and vetted solutions.

In order to allow for responsiveness and flexibility during the pandemic period, schools may use and/or acquire technology solutions from companies who have signed the student privacy pledge in lieu of a formal data sharing agreement. Waiving of a data sharing agreement is only during the time that HIDOE schools are conducting remote learning. Upon return to normal in-school operations, schools that plan to continue use of the acquired solution will need to enter into a formal data sharing agreement from the company. For more information, contact HIDOE's Data Governance and Analysis Branch.

**Training and Assistance**

HIDOE-developed information and support sites are available to staff. The sites are updated as new information, training, FAQs, etc. are received.

- **Google at HIDOE**: This site provides information about HIDOE's enterprise Google tenant, including recordings of training sessions, FAQs, and News/Updates on the ongoing Google migration project.
- **Webex at HIDOE**: This site provides information about HIDOE's centrally-managed Webex application. The site provides an overview of the various "modules" – Webex Meetings, Webex Teams, Webex Training, Webex Events, as well as FAQs, training videos, and other information and announcements.
- **HSTE Training in April 2020**: HIDOE is partnering with the Hawaii Society for Technology in Education (HSTE) to provide a series of professional development sessions on Webex and Google Meet. Sessions are being recorded and links are posted to the training schedule.
- **HIDOE Training in April/May 2020**: HIDOE is also developing training sessions during the month of April/May and will be announcing sessions when they are scheduled.

In addition to the informational websites, HIDOE staff may also contact the IT Help Desk for questions about the application or need login or password assistance. HIDOE staff may submit a ticket online using ServiceNow at http://help.hidoe.org (*employee login required*), or by calling the IT Help Desk Monday through Friday from 7:45 a.m. to 4:30 p.m. at (808) 564-6000, or for neighbor islands, via HATS at 8-1-808-692-7250.

**Using Zoom for E-Conferencing**

HIDOE staff have raised questions about using the online meeting software Zoom. While Zoom can be FERPA compliant, it is only compliant when entered into the proper contractual agreements with the company. HIDOE has not yet implemented a contractual relationship with the company for department-wide use. For individual schools that have a contractual agreement and data sharing agreement with Zoom, they may move forward with using the application and follow the guidance provided in this section. For those using a free version of Zoom, they should be aware that the free version does not have the standard security measures and does not protect student privacy. All HIDOE staff have access to Webex and Google's Gsuite for Education that are centrally provisioned and managed by HIDOE's Office of Information Technology Services. Webex and GSuite have both been implemented in line with privacy and security compliance while also ensuring that these products can scale to meet the needs of HIDOE's increasing bandwidth demands. These products also provide a single point for staff to sign into the applications (i.e., single sign-on/SSO) by using their HIDOE-issued account (@k12.hi.us). HIDOE is currently seeking to acquire Zoom via a contractual agreement so that staff can use this video-conferencing application while ensuring the privacy and safety of our students and staff while online.

**Reminders and Guidance on Student Privacy while Online**

The purpose of e-conferencing is to connect students and teachers in an online meeting to conduct conversations and the transferring/sharing of educational material when the ability to do it face-to-face is unavailable. Adherence to student privacy policies and regulations should be followed in any classroom environment. The following are reminders about student privacy:

- If there is a need to take home personal information about students when switching to virtual instruction, staff can take home this information as long as they have a legitimate educational interest in the education records, as determined by their educational agency or institution.

- School officials, including educators, who take education records home are prohibited from further disclosing personally identifiable information (PII) from the education records, except as otherwise permitted under the Family Educational Rights and Privacy Act (FERPA); and, should use reasonable methods to protect the education records, and the PII in those records, from further disclosure. These protections can include access controls that are physical, technological, and administrative controls.

- The use of e-conferencing applications to hold virtual classes and provide instruction does not generally constitute a disclosure of education records protected by FERPA. Similar to an

in-person class, educators should avoid disclosing PII from educational records. As a general practice, educators should:

- Ensure that access to the virtual class is secure and limited to those who are participants in the class.
- Ensure that links to access the class are kept confidential and limited to those participating in the class.

- Assuming that during a virtual class, PII from education records is not disclosed, non-students can observe a virtual class. However, US DOE Student Privacy Policy Office recommends that schools should discourage non-students from observing virtual classrooms in the event that PII from a student's education record is, in fact, disclosed in such virtual classrooms.
  - Under FERPA's general consent rule, prior written consent is required before PII from a student's education record may be disclosed. FERPA's directory information exception permits certain PII from education records to be disclosed during classroom instructions to students who are enrolled in and attending a class. However, if a parent or guardian of a student has "opted out", directory information about a student may not be shared without prior written consent. Schools administrators would know if any student has "opted out."
  - In Hawaii, directory information includes the following information: the student's name, date and place of birth, address, telephone, dates of attendance, class level, major field of study, participation in officially recognized activities, and sports, weight and height if member of an athletic team, awards received, graduation date, and the most recent previous educational agency or institution attended.

- In order for students to appear on camera (video or audio), a signed "Student Publication Audio Video" (SPAV) form allowing HIDOE to use student images, video, etc. in school publications can appear on video and/or audio should be on file for the student(s). Students who do not have a signed SPAV form should not appear on camera (video or audio). Alternate teaching methods should be used for students who do not have a signed SPAV on file.
  - Schools should also be entering SPAV permissions forms into HIDOE's student information system (Infinite Campus). Information can be found under the *Student Privacy* tab.
  - If the *Student Publication/Audio/Video* field is marked as "Y: Yes", permission has been given to allow the student to be photographed,video taped, etc.

- In general, recording virtual class sessions is allowable as long as the video does not disclose PII from students' education records during the virtual class session, FERPA would not prohibit the educator from recording.
  - Video recordings of virtual classroom lessons qualify as "education records" protected under FERPA only if they directly relate to a student and are maintained by an educational agency or institution or by a party acting on their behalf. FERPA's nondisclosure provisions may still apply to such video recordings even if they do not qualify as "education records," if the video recording contains PII from student education records.

- If class sessions will be recorded, all students and their parents or guardians should be aware. Notification should also include the purpose of the recording and who will have access to the recording. For example, the recording will be available for students who missed the lesson. Generally, students and school administrators will have access to the video.

- Before conducting one-on-one conversations, it is recommended that staff and educators review their relevant policies and standards related to communicating with students. Otherwise, approved methods for communication should be used (e.g., work email address, not a personal one, etc.). The content of the intended conversation also determines the best way to proceed. Answering content-related questions or providing one-on-one help likely does not implicate any privacy laws. If the purpose is to discuss information from education records (e.g., discussing issues with grades), extra care should be taken to ensure that the conversation is private (e.g., asking that other individuals in the home not be present). Educators may consider holding virtual office hours (i.e., have a specific set of hours where they will be available to students via web conference to answer questions).

- Staff and educators should refrain from posting student photos and names on social media, including those of the entire class together on a web conference.
  - If while teaching, the educator took a picture, video or audio recording of their student or students, the recording can be considered an educational record and the educator should not post the picture or recording on social media accounts.

**E-Conferencing Best Practices and Guidance**

Even the most secure e-conferencing application can let in uninvited or unwanted participants if sessions are not set up correctly or have certain features enabled that can be used if uninvited/unwanted participants get into the session. The following are some general best practices and guidance to help create a more secure online experience for staff and students:

- Do not make meetings or virtual classrooms public: Unless your session is meant for public viewing or participation, avoid posting e-conferencing session links publicly (including any passwords to enter the session).
  - Some e-conferencing applications have personal meeting rooms or sessions. These types of rooms and sessions are basically one continuous ongoing session that anyone with the room or session information can join at any time. Avoid using these types of personal rooms and sessions for public viewing.

- Password protect meetings: Adding passwords to meetings help to protect against uninvited guests and to secure meeting information.
  - In addition to passwords, some e-conferencing applications have features for having participants register so that only registered participants are allowed to access a session.

- Be aware of your surroundings: With the camera and/or microphone on, meeting participants will be able to see and hear what is going on in your surroundings. Physical surroundings could

have people talking in the background or people walking around the room and appearing on the video feed.

- Seek as quiet a space as possible with no or minimal background noise.
- Some e-conferencing applications have a feature to change or blur backgrounds. If the feature is available on the e-conferencing application being used, this is an option to block out certain background views.
- Adjust the camera position and distance so that as little background is visible and the focus is on the host/participant, or limit the ability for anyone to walk behind the host/participant and appear on video.

- Announce recording of sessions: As a courtesy to meeting participants, if a session will be recorded, announce this to the participants at the start of the meeting. Explaining why the meeting is recorded and what it will be used for is also helpful.
  - In order to ensure student privacy, academic property, and copyrights, it should also be announced that students and parents who are participating or viewing the session, not copy or record it for subsequent posting to social media, etc.

- Disable *join before host* feature: Many e-conferencing applications have a feature that allow for participants to join before the host does. Disabling this feature will make participants wait until the hosts starts the session so that participants (invited and uninvited) cannot interact with each other prior to the host joining.

- Disable *file transfer* feature: For e-conferencing applications that allow for file transferring, disable this feature if file transfers are not needed as it will minimize the possibility of digital virus sharing.

- Manage *screen sharing* options: Many e-conferencing applications allow participants to share their screens during a session and, for some, the application enables screen sharing as a default. If there is no need for participants to share their screens, the host should consider disabling this option for the session.
  - Anyone who will be sharing screens during a session should close any unnecessary applications, documents, windows, etc. to minimize accidentally sharing something that should not be shared.
  - When possible, it is better to share only the needed application(s) instead of the entire screen.

- Manage participants: e-conferencing applications have features to assist the host with managing participants during a session. These features are helpful in the event uninvited or disruptive participants log in.
  - Lock meetings/sessions: if a locking feature is available, hosts can lock the meeting once it has started. Hosts should keep in mind that this also locks invited participants out as well. Some applications also have a waiting room feature that puts participants in a separate virtual room/space until they are admitted to the session by the host.
  - Remove uninvited or disruptive participants: many of the most common e-conferencing applications allow a host to remove or expel participants from a meeting. Depending on

the application, this feature will need to be used in combination with the session locking features or removed/expelled participants may be able to rejoin the session.
    - Mute participants: the majority of the e-conferencing applications allows hosts to mute participants, as well as to mute all participants upon entry. Some applications even have a *raise hand* feature so that the host can unmute specific participants who wish to speak.
    - Only use video when needed: sometimes e-conferencing applications also serve as a conference call line or conference bridge. In these cases, video will likely not be needed and should be disabled if the application allows. This not only ensures that participants do not show any unwanted or disruptive content on their camera, but also saves on bandwidth resources.

- In the event an e-conferencing session gets hacked or bombed by an uninvited guest, the host should:
    - focus first on kicking the person out or even shutting down the meeting temporarily if necessary.
    - then, contact and notify the following:
        - the school principal or office director/administrator
        - the Office of Information Technology Services (OITS) technology security team at eab@k12.hi.us
        - HIDOE's Communications at (808) 784-6200 or via email at doeinfo@k12.hi.us.

- Students should report any incidents of cyberbullying to the teacher, counselor, or administrator.
    - Secondary school students also have the option to report bullying via HIDOE's bullying reporting app (https://www.speaknowhidoe.com/). The app also allows for anonymous reporting.

**Technical Considerations When Using E-Conferencing**

When working outside of an office environment, technical factors could be significantly different than what is available in the workplace. The following are a few technical considerations when using e-conferencing applications:

- If connecting and participating from a laptop, plug the laptop into an outlet (preferably one with a surge protector); battery use and low battery availability can adversely affect the quality of video and voice.

- If connecting from a home network and personal internet plan, be aware that some plans (especially entry-level ones) may not provide as much bandwidth speed. For plans with a data cap, some internet service providers may throttle bandwidth as usage is nearing or exceeds the data cap.
    - Also be aware of the number of people on the home network at one time. In a work-at-home or stay-at-home situation, many families are online at once which could be more than what a home network can manage.

**IEP Meetings via E-Conferencing**

The following guidance was provided in a March 2020 memo on conducting virtual IEPs:

In an effort to ensure the rights of students with disabilities under the Individuals with Disabilities Education Act (IDEA) and Hawaii Administrative Rules Chapter 60, schools may continue to conduct eligibility, evaluation, and IEP meetings through remote means when appropriate. The HIDOE leadership recognizes in this unique and ever-changing circumstance that schools can only make a good faith effort to meet the timeline requirements.

Schools shall conduct IEP meetings virtually using secured Webex or conference calls. In the case where a parent(s)/legal guardian(s) or any other team member does not have online platform capabilities, they may call into the virtual meeting via telephone.

If an evaluation of a student with a disability requires a face-to-face assessment or observation, the evaluation must be delayed during the facility's closure. Initial evaluations and reevaluations that do not require face-to-face assessments or observations may take place during the school closure. If sufficient information is available for program purposes and eligibility is not in question, then assessments may be determined unnecessary by the IEP Team. A reevaluation may be considered or requested at any future time should the situation warrant.

Considerations for virtual IEP meetings:

- Engage in ongoing open communication with parent(s)/legal guardian(s) by supporting their communication needs as much as possible.
- Provide IEP Team members with necessary documents via email or standard mail when needed.
- Take all necessary cautions to ensure the meeting place is private.
- Do not use personally identifiable information in the title of the virtual meeting.
- Plan ahead as much as possible to allow all team members an opportunity to prepare.
- Meeting time and means must be mutually agreed upon with the parent(s)/legal guardian(s).
- Given a long-term closure, when the team does not have updated and accurate performance data, and there are no proposed revisions to the current IEP, it may not be feasible to conduct an annual review of the IEP. In this case, the school administrator, teacher, and parent(s)/legal guardian(s) should discuss the situation and may need to consider a mutually agreed upon extended timeline.

Note: Schools are still responsible for documenting the IEP meeting, and students can be a participant.

**Additional Resources**

| | |
|---|---|
| Student Privacy Resources | US DOE's Privacy and Technical Assistance Center (PTAC) Webinar Recording: FERPA and Virtual Learning https://studentprivacy.ed.gov/training/ferpa-and-virtual-learning-during-covid-19-webinar-recording |
| | PTAC: Slidedeck FERPA and Virtual Learning: https://studentprivacy.ed.gov/resources/ferpa-and-virtual-learning-during-covid-19 |

| | |
|---|---|
| | |
| | PTAC: FERPA & COVID-19 FAQs https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions.pdf |
| | PTAC: When is a photo or video of a student an education record under FERPA? https://studentprivacy.ed.gov/faq/when-photo-or-video-student-education-record-under-ferpa |
| | PTAC: Regarding Surveillance Video of Multiple Students https://studentprivacy.ed.gov/resources/letter-wachter-regarding-surveillance-video-multiple-students |
| | HIDOE's Quick Guide to FERPA: http://www.hawaiipublicschools.org/DOE%20Forms/DataGov/FERPABrochure.pdf |
| | HIDOE's Parent Notification and Guide to Student Information Privacy in Hawaii's Public School: http://www.hawaiipublicschools.org/DOE%20Forms/DataGov/ParentNotification.pdf |
| | HIDOE's Student Privacy Website: bit.ly/FERPAHI |
| | PTAC's website: https://studentprivacy.ed.gov/ |
| Webex Resources | HIDOE: https://sites.google.com/k12.hi.us/webex *Includes system requirements to use Webex* |
| | HSTE: https://docs.google.com/document/d/1D6srs9UPL6JpmZ6Jp1Waknmyvn13BoyEhCW1kJ56iak/edit |
| | WEBEX: https://www.webex.com/webexremoteedu.html |
| Google Resources | HIDOE: https://sites.google.com/k12.hi.us/gsuite/ *Includes system requirements to use Google video conferencing* |
| IEP Information | HIDOE Memo: Programming and Timelines for Students with Special Needs During School Closures (3/27/20) |
| Blackboard Resources | HIDOE: https://hidoe.blackboard.com/ |
| | Technical Requirements: https://help.blackboard.com/Learn/Student/Getting_Started/Browser_Support |

## PARTNER AND COMMUNITY SUPPORT *As of 4/15/20*

**Introduction**

Community and corporate organizations have been instrumental in helping education agencies, like HIDOE, address technology needs during the COVID-19 pandemic.

**HSTE Training on Webex and Google Meets**

HIDOE is partnering with the Hawaii Society for Technology in Education (HSTE) to provide a series of professional development sessions on Webex and Google Meet. Sessions are being recorded and links are posted to the training schedule.

**Charter/Spectrum Free 60-day Broadband Internet and WiFi Offer**

- Beginning on March 16, 2020 Charter Communications is offering free Spectrum broadband and Wi-Fi access for 60 days to households with K-12 and/or college students who do not already have a Spectrum broadband subscription and at any service level up to 100 Mbps.
- On March 25, 2020, Spectrum issued a press release indicating that the offer for 60-day broadband access has been expanded to include educators who do not already have Spectrum broadband subscriptions.
- For more information: https://corporate.charter.com/newsroom/charter-expands-free-60-day-spectrum-broadband-internet-and-wifi-offer-to-include-educators-who-are-new-spectrum-subscribers

**Hawaiian Telcom Free 2-month Internet Service**

- Beginning March 14, 2020 Hawaiian Telcom is offering free internet services two (2) months of free Internet service to households with K-12 and/or college students who currently do not subscribe to Hawaiian Telcom Internet service.
- Educators may contact Hawaiian Telcom to see if they are eligible to receive two months of internet service if they currently do not subscribe to Hawaiian Telcom Internet services.
- To sign up, contact Hawaiian Telcom at 643-8888.

**T-Mobile EmpowerED 2.0 Program**

- T-Mobile's EmpowerEd program offers wireless devices and service plans to eligible schools and their students.
  - Participating schools can receive up to $200 per student to put toward mobile internet devices, including hotspots, laptops, and tablets.
  - A 2-year contract is required on a qualifying unlimited plan for $20 per month.
- For more information: https://www.t-mobile.com/business/education/empowered2
- For schools purchasing devices through this program, please make sure to submit a telecom request and that the device has content filtering abilities.

**NOTE: The above listing of technology offers is not an endorsement by HIDOE of any product or service.*

## ELECTRONIC SIGNATURE *As of 3/23/20*

**Introduction**

- The use of electronic signature through Adobe Sign is available to HIDOE staff.
- The use of electronic signature is valid and enforceable in most cases under the United States' Electronic Signatures Act (2000) and Hawaii Revised Statutes (HRS 489E-7).

**Accessing Adobe Sign**

- Instructions for accessing and using the Adobe Sign product can be found online: https://sites.google.com/k12.hi.us/adobe-e-sign/resources *(employee login required)*
- Staff will need to log in using their @k12.hi.us account and password – the same one used to log into your enterprise Google account.

**Processes and Procedures When Using Adobe Sign**

- There are several different types of electronic signatures available through the Adobe Sign product.
  - Digital replica
    A digital replica is a digital copy of an actual signature, which can be added either by uploading a scanned copy of a signature or by signing the document on a device that has touchscreen and handwriting capabilities. The following is an example of a digital replica:

    
  - Font-based
    A font-based signature is one that is a typed name that is in an italics or handwriting font style. The following is an example of a font-based signature:
    *Jane Doe*
- Users should check with the office that issues or processes the form to ensure that electronic signatures are acceptable or if an actual "ink" signature is needed. If a digital signature is acceptable, users should also check if a certain type of signature (i.e., digital replica or font-based) is acceptable.
- Anyone using electronic signatures on documents should ensure that current HIDOE processes and procedures are followed (similar to if it were done via "ink" signature), unless otherwise instructed to do so. This will include (but is not limited to):
  - Both the originator and those signing the document should track is routing progress.
  - If a policy, procedure, or guideline requires that a hard copy of the signed document be kept on file, a copy should be printed and filed in the appropriate office(s).
  - If a policy, procedure, or guideline requires a hard copy to be submitted (even if an electronic signature is acceptable), a hard copy should be printed and provided accordingly.

- If a policy, procedure, or guideline requires a hard copy for audit purposes, a hard copy should be printed and submitted accordingly.

**Restrictions on Use**

- The use of electronic signature is only for signatures of HIDOE staff. Currently licensing agreements do not allow for electronic signatures outside of HIDOE (i.e., no parent signatures, no contractors/vendors, etc.).
  - Any costs incurred for incorrect use of the current licensing agreement will be paid by the office/school that generated the cost and access may be restricted or revoked for the user(s).
- Anyone using electronic signatures should check with the office that issues or processes the form to ensure that electronic signatures are acceptable or if an actual "ink" signature is needed.
- If a digital signature is acceptable, users should also check which type of signature (i.e., digital replica or font-based) is acceptable.

**Retention of Documents**

- Digital/Electronic documents should follow the same retention schedule as paper documents. Schedules are available on the Hawaii State Archives website: https://ags.hawaii.gov/archives/about-us/records-management/records-retention-and-disposition-schedules/
- Users should be aware that Adobe Sign does not allow users to delete any documents once they are uploaded. This includes documents that are still in draft mode or have been completed and signed.

**Additional Resources**

- An overview/tour of the Adobe Sign product can be found online: https://www.adobesigndemo.com/en/demo/send
- HIDOE Adobe Sign information site: https://sites.google.com/k12.hi.us/adobe-e-sign/home

**Assistance**

- For assistance, please submit requests at any time online using ServiceNow at http://help.hidoe.org *(employee login required)*. You may also call the IT Help Desk Monday through Friday from 7:45 a.m. to 4:30 p.m. at (808) 564-6000, or for neighbor islands, please use the HATS line at 8-1-808-692-7250.

## AVOIDING SCAMS & FRAUD DURING EMERGENCY SITUATIONS *As of 3/18/20*

**Introduction**

Scams are prevalent on a regular basis. Unfortunately, natural disasters and emergency situations often result in increased scams by those who are looking to make money or leverage confidential information to their benefit. It is important to exercise caution when reading emails, visiting websites, making charitable donations, etc.

**Be Careful of Phishing Attempts**

- Phishing is a tactic that is used to persuade individuals to provide sensitive information and/or take action through seemingly trustworthy communications.
  - Target(s) may be contacted via email, telephone, text messages, or social media sites by someone posing as a legitimate person or institution.
  - In some cases, phishing attempts can lead to identity theft and financial loss.
- In general, phishing attempts fall into three categories – phishing, spear-phishing, and whale-phishing (also known CEO Fraud).

| | Phishing | Spear-Phishing | Whale-Phishing (CEO Fraud) |
|---|---|---|---|
| **What method is used?** | Broad/Mass communication | Targeted communication | Targeted communication |
| **Who is targeted?** | Broad audience | Specific groups of staff or organizations | High-level, highly-visible people (e.g., executives, politicians, etc.) |
| **How do they attack?** | ▪ General communication<br>▪ Sometimes automated<br>▪ Not very sophisticated<br>▪ Usually obvious | ▪ Targeted communication<br>▪ Appears to have information specific to the organization, "insider information", or information from social media<br>▪ Advanced techniques<br>▪ Harder to detect and identify | ▪ Targeted communication to executive(s)<br>▪ May impersonate an executive and target others in the organization or direct reports<br>▪ Appears to have information specific to the organization, "insider information"<br>▪ Advanced techniques<br>▪ Harder to detect and identify |
| **What are they after?** | ▪ Usernames<br>▪ Passwords<br>▪ Financial details<br>▪ Personal information | ▪ Organization information<br>▪ Access to organization systems<br>▪ Confidential information | In addition to spear-phishing:<br>▪ Personal/Business information of executives or direct reports |

| | | | |
|---|---|---|---|
| | | | ▪ Direct action (e.g, money transfers, granting access, etc.) |

**Use Caution with Email Messages**

- Only reply to email from senders you know and can confirm.
  - The sender's display name can be changed to impersonate anybody. To better identify whether the email is legitimate, look at the sender's full email address.
  - The "reply to" field can be redirected anywhere. If you do reply, make sure you know where it is going before you send it.
- If the email contains links, make sure you know where the link goes.
  - Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs .net).
  - For links that do not have the URL listed, hovering the computer mouse or cursor over the link usually displays the URL the link is directed to.
- Only open attachments if you are certain of the person who sent them and you requested or expected to receive them.
- Look for spelling and grammatical errors.
  - Malicious emails tend to have spelling mistakes and poor grammar.
- Be suspicious of emails that try to instill a sense of fear or urgency such as financial penalties, credit card cancellations, account closures, etc.
- Be suspicious of emails asking for personal or confidential information (e.g., social security numbers, financial information, etc.).
- Be suspicious of emails asking for company information.
  - Do not provide confidential information or information about your organization, including personnel, operational procedures, security, or networks unless you are certain of a person's authority to have the information.
- Disable automatic email attachment downloads on your device.
  - To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it.

**Be Aware of Websites**

- Avoid clicking on links embedded in an email message.
  - Even if the message was sent from someone you trust, it is best to type the link into your browser
- Look for signs of legitimacy.
  - Check if the website lists contact information and validate it.
- Read the URL carefully.
  - Check the spelling of the website since malicious websites often appear almost identical to the spelling of the site you are trying to visit.
- Check where links are directed.

- Depending on the device, hovering or right-clicking on the hyperlink will reveal the true destination of the link.

**Be Aware of Solicitations for Donations**

- You don't have to give donations over the phone. Don't let any caller pressure you. Take time to do the research.
- Ask the fundraiser for the charity's exact name, web address, and mailing address, so you can confirm it later. Some dishonest telemarketers use names that sound like large well-known charities to confuse you.
- The safest way to give on social media or through crowdfunding is to donate to people you know who contact you about a specific project.
  - Don't assume solicitations on social media or crowdfunding sites are legitimate, or that hyperlinks are accurate — even in posts that are shared or liked by your friends. Do your own research.
- Be careful how you pay.
  - Charitable organizations do not ask for payment by gift cards or wire transfers.

**Reporting Suspicious Email**

- If you receive any suspicious email on your work email account, please forward the message(s) to phishing-report@k12.hi.us

**Resource Sites**

- U.S. Department of Homeland Security https://www.dhs.gov/
- Federal Trade Commission https://www.consumer.ftc.gov
- Phishing.org https://www.phishing.org/
- Stay Safe Online https://staysafeonline.org/

## OFF-SITE/REMOTE ACCESS FOR WORK (TELEWORK) *As of 3/18/20*

**Introduction**

- In the event of a need to work from an off-site location, there are steps users should take to ensure a more secure computing experience.
- Information in this section provides guidance for two scenarios:
  - For users who are using HIDOE-issued devices
  - For users who are using their own personal devices
- For offices that have technology staff support, please check with the support staff before attempting to check, install, or update anything on your HIDOE-issued device.
- If using a personal device, the device should meet the standards of a HIDOE-issued device. However, please check that any updates or installations do not conflict with the applications and services already installed on the personal device. If a personal device cannot meet the same standards as a HIDOE-issued device, please contact the office supervisor regarding moving forward with telework options.

**General Statement on Security and IT**

- Security measures while teleworking should cover information systems and technology, as well as all other aspects of information used or accessed by employees including (but not limited to):
  - paper and hardcopy documents
  - other media with confidential or personally identifiable information
  - storage devices
  - telecommunications equipment (e.g., cell phones, tablets, laptops, etc.)
- It is important to remember that although employees are working from home or from another approved location, employees are still responsible to protect and manage records and other sensitive information they have in their possession and/or are transmitting across external networks.
- Employees who are working from home or from another approved location must remain sensitive to individual rights to personal privacy and comply with all federal, state, and HIDOE regulations and policies, including:
  - FERPA (Family Educational Rights and Privacy Act)
  - IDEA (Individual with Disabilities Education Act)
  - USDA (US Department of Agriculture; for free and reduced-cost lunch information)
  - HIPAA (Health Insurance Portability and Accountability Act; for health data not covered under FERPA)
  - HRS §487J (personal information protection requirements)
  - HRS §487N (security breach of personal information)
  - HRS §487R (destruction of personal information records)
  - HAR §8-34 (Protection of Education Rights and Privacy of Students and Parents)

**Important Note on System Compatibility**

- HIDOE has several legacy systems that may not be compatible with certain updates and versions. Employees should check the online compatibility matrix frequently:

https://intranet.hawaiipublicschools.org/offices/oits/esb/Documents/Software%20Compatibility%20Matrix.pdf#search=compatibility%20matrix

**Device Security**

- Antivirus Software: Make sure there is antivirus software installed on the device and it is up-to-date.
  - HIDOE-issued devices should already have antivirus software installed.
  - To check if the device has antivirus software:
    - Windows devices
      - Click on the Windows Start icon, and in the Search programs and files text box, type "Programs and Features" and click ENTER.
      - Malwarebytes is installed if they are in the program list:
        - Malwarebytes Endpoint Agent
        - Malwarebytes Endpoint Agent and .Net system prerequisites installer *(only appears if the device does not have the minimum required .NET installed)*
    - MacOS devices
      - Click on the *Launchpad* icon
      - Type "terminal" in the search bar to locate the *Terminal* application
      - Open the *Terminal* application
      - Enter the following into the terminal application:
        **kextstat | grep com.malwarebytes**
      - If the following appears on the output Malwarebytes was installed incorrectly and needs to be reinstalled:
        **ELI-01:"~ tcadmin$"**
    - Mobile devices (iOS devices, android devices)
      - Anti-Virus/Anti-Malware can be downloaded from the Apple App Store or the Google Play Store
      - McAfee, Lookout, AVG, Symantec, and Avast are the more common anti-virus applications that are safe to use.
      - Be cautious of downloading and using anti-virus applications that are unfamiliar.
      - Avoid downloading apps from third-party app stores.

  - If antivirus software is not installed on the HIDOE-issued device, the software can be downloaded and installed from the following site *(employee login required)*:
    - Windows devices
      https://intranet.hawaiipublicschools.org/offices/oits/eisb/Pages/Malwarebytes-Endpoint-Protection-for-Windows.aspx
    - MacOS devices
      https://intranet.hawaiipublicschools.org/offices/oits/eisb/Pages/Malwarebytes-Endpoint-Protection-for-Mac-OS.aspx
    - Chromebooks

No antivirus software is needed. Chromebooks come with built-in virus protection as part of the ChromeOS.

- Operating System Security Updates: Make sure operating system security updates are current on the device.
  - Microsoft, Apple, and Google periodically issue security updates or patches for their operating systems. In many cases, these updates will be applied automatically, depending upon the settings configured on the device.
  - To check the update status on the device and install any available updates:
    - Windows devices (for Windows 10)
      - Select the Start button, and then go to Settings > Update & Security > Windows Update > Check for Updates
      - If updates are available, follow the on-screen instructions to install them and reboot your computer.
      - If your computer is set to automatically perform updates, please ensure it is on the latest version (Windows Update will display the message "You're up to date" if you have the latest updates installed).
    - Macintosh/Apple (for MacOS Mojave or later)
      - Choose System Preferences from the Apple menu, then click Software Update to check for updates.
      - If any updates are available, click the Update Now button to install them. Or click "More info" to see details about each update and select specific updates to install.
      - When Software Update says that your Mac is up to date, the installed version of MacOS and all of its apps are also up to date.
      - To automatically install MacOS updates in the future, including apps that were downloaded separately from the App Store, select "Automatically keep my Mac up to date." Your Mac will notify you when updates require it to restart, so you can always choose to install those later.
    - Chromebook
      - Chromebooks manage updates automatically so Chromebooks are always running the latest and most secure version (some HIDOE-issued Chromebooks will be configured to update to the latest HIDOE-supported version for application compatibility). These updates will be installed and applied automatically.
    - iOS devices (e.g., iPhone, iPads, etc.)
      - To check if you have updates to install go to:
        Settings > General > Software Updates
        If you have updates to install there will be a "Download and Install" option. Follow the instructions to install the updates.
    - Android OS devices (device type varies)
      - To check if you have updates to install go to:

Settings > System Updates > Check for new system update
If there are no updates you will see a message "Your device is up-to-date".
If you have updates follow the instructions to install the updates.

- Other Updates: In addition to updated antivirus and operating systems, users should also ensure the following are up-to-date:
  - Web browsers
  - Email clients
  - Instant messaging clients
  - Office productivity software (e.g., document viewers, word processors, spreadsheet tools, etc.)

**Accessing HIDOE Systems**

- Some of HIDOE's modern cloud-based systems (e.g., Google, Infinite Campus, etc.) are accessible outside of the office and already have secure connections. However, there are certain HIDOE systems and applications that can only be accessed on the HIDOE network. To access these systems, VPN (virtual private network) access will be needed.
  - See section on *HIDOE VPN (Virtual Private Network)*.
- Employees should avoid using public and unsecured networks.

**Beware of Scams**

- Scammers may contact employees via email, text, SMS, phone, or social media, and may pretend to be a trusted colleague or an executive in the organization. Scammers may seek sensitive information, payments, gift cards, etc. Even if the phone number or email address is recognizable, be sure to confirm every request for sensitive information via a trusted means of communication.
- Be aware of malicious websites posing as official or credible sites. Such sites may contain viruses, etc.

**Additional Resources**

- Chromebook Security Page: https://support.google.com/chromebook/answer/3438631?hl=en

**Assistance**

- For assistance, please submit requests at any time online using ServiceNow at http://help.hidoe.org *(employee login required)*. You may also call the IT Help Desk Monday through Friday from 7:45 a.m. to 4:30 p.m. at (808) 564-6000, or for neighbor islands, please use the HATS line at 8-1-808-692-7250.

## HIDOE VPN (VIRTUAL PRIVATE NETWORK) *As of 3/23/20*

**Introduction**

HIDOE employees who need to access systems and applications that are only accessible on the HIDOE network may request VPN access. The current VPN software used by HIDOE is Cisco AnyConnect Secure Mobility Client.

**HIDOE Systems and Applications**

Some of HIDOE's modern cloud-based systems (e.g., Google, Infinite Campus, etc.) are accessible outside of the office and already have secure connections. However, there are certain HIDOE systems and applications that can only be accessed on the HIDOE network. To access these systems, VPN (virtual private network) access will be needed. Access to HIDOE Systems and Applications require appropriate permissions.

- A list of HIDOE cloud-based systems and applications that are currently using HIDOE's active directory for single sign-on is available in ServiceNow *(employee login required)*: https://hidoe.service-now.com/kb_view.do?sysparm_article=KB0011207

- HIDOE systems requiring VPN access can be found in the HIDOE ServiceNow knowledge base *(employee login required)*: https://hidoe.service-now.com/kb_view.do?sysparm_article=KB0011460

- Specific notes and information on certain systems:
  - eCSSS: HIDOE's electronic comprehensive student support system (eCSSS) can be accessed remotely the way it is accessed at the work site.
  - FMS: HIDOE's financial management system (FMS) must be accessed via remote desktop connection (i.e., an off-site device connecting to the device located in the work place). Even with remote access, documents printed from FMS will still print to the work site printer that is designated for FMS printing.
  - Time & Attendance (Kronos): HIDOE's time and attendance system must be accessed via remote desktop connection.

  *Note: For remote desktop connections, instructions for resetting the PIN are available here.*

**Requesting VPN Access**

HIDOE employees who need to access systems and applications that are only accessible on the HIDOE network may request VPN access.

- Employees who do not have VPN access and need it to work off-site should:
  - download the VPN Request Form *(employee login required)*: https://intranet.hawaiipublicschools.org/offices/oits/eisb/Documents/DOE VPN Access Request Form.docx

- Complete the form and have the appropriate administrator sign the “Sponsor” section (e.g., Director, Principal, Complex Area Superintendent, or Assistant Superintendent)
- Email the completed and signed form to vpnrequest@k12.hi.us.
- Instructions to fill out the form and step-by-step installation and use instructions for the VPN are available at: https://hidoe.service-now.com/kb_view.do?sysparm_article=KB0011466

## NETWORK CONNECTIVITY & CONTENT FILTERING *As of 4/15/20*

**Network Connectivity**

- HIDOE Network
  - For employees who continue to work from office locations, HIDOE's network connectivity will continue to be available.
  - Network traffic and usage will be monitored. As schools and offices move to remote work locations (e.g., telework, etc.) and online learning, adjustments will be made to network resources as necessary.
- Other Network Connections
  - Internet service providers have been offering special discounts and other services to families with K-12 students, as well as for educators.
  - See *Partner and Community Support* section.

**A Note on Content Filtering**

- HIDOE complies with federal regulations and uses content filtering on its student network to ensure a safe and security online experience for students.
- Schools moving to online learning from remote/non-school locations, school staff, parents, and guardians need to be more aware of what students are viewing and accessing online, especially if the device the student is using does not come with content filtering at the device level or some sort of parental controls over content.
- Additional information is available on keeping children safe while online at home.
  - **HIDOE Child Internet Safety Resources**: Flyer containing guidance and tips from the Hawaii Attorney General's Office, as well as information about enabling safety features and parental controls on devices.
  - **Digital Citizenship – Appropriate Media Use**: Flyer containing information from commonsense.org about appropriate media use for children to provide a safe online experience.

## INFINITE CAMPUS *As of 4/1/20*

**Introduction**

During the COVID-19 pandemic, changes may be made to attendance, grading, and other areas that will also change how schools enter information into HIDOE's student information system – Infinite Campus.

**Student Attendance**

This information and instructions are being provided to address attendance records in HIDOE student information system (Infinite Campus). It is provided specifically to address the COVID-19 situation and will be updated as the situation progresses. Schools who are not using HIDOE's Infinite Campus system, should work with their administration to determine appropriate dates and actions required to update their system(s).

- Recommendations for Schools during COVID-19 Statewide Shutdown
  - The Office of Information Technology Services (OITS) will be responsible for updating the schools' Calendar settings so attendance cannot be taken in Infinite Campus.

  - If not already completed, schools need to print their Attendance Report prior to OITS updating their Calendar. Schools may choose to use ONE of the following. If the report(s) show zero records, that indicates that the school does not have any future attendance entered, and nothing further needs to be done:

    - The Daily Attendance report (an instructional document is provided).
    - The following two Ad Hocs that have been created:
      - student ***ATTENDANCE – School Closure (ALL CODES)
      - student ***ATTENDANCE – School Closure (SUS/ISS/CH19)

    Path: Ad Hoc Reporting > Data Export > Elem Advanced Clerk/Secondary Registrar folder > student ***ATTENDANCE – School Closure (ALL CODES) or student ***ATTENDANCE – School Closure (SUS/ISS/CH19).
    **Please make a COPY of the Ad Hocs and DO NOT EDIT. Save in PDF or CSV format.**

- **[Completed]** For March 23-25, 27; March 30-April 3, April 6. (March 26 is Kuhio Day- state holiday). OITS updated School Calendars on Monday, March 30.
  - Calendars were set to "Admin Emergency" for March 23-25, 27; March 30-April 3, April 6.
  - Calendars were set to School Day for days when teachers are required to report to work (currently March 23-25, 27 and April 6). These days will not be Instructional days, and will not be Attendance days because students are not required to attend.

- For April 7 to April 30:
  - For this time period, OITS will update School Calendars on **Thursday, April 16, 2020**.
  - Day Events in Calendars will be set to "Admin Emergency."
  - Calendars will be set to School Day. These days will not be Instructional days, and will not be Attendance days because students are not required to attend.

- **If dates change due to COVID-19 updates, OITS will continue to make the corrections for Infinite Campus schools.**
- Schools will update their attendance to reflect student attendance that needs to be carried on, such as suspensions using their printed Attendance Report. Refer to the Ad Hoc reports above.
- OITS will work with the 3 Multi-track schools.
- Hawaii Public Charter Schools not using the DOE Calendar would be responsible for updating their Calendar.