St. Helena Catholic School

Chromebook Policy

2018-2019

Este año St. Helena tendrá una estación de computadores Chromebooks para alumnos de 4° y 5° grado. Cada alumno recibirá un Chromebook para el uso en la aula. Los profesores usarán Chromebooks para la enseñanza de temas tecnológicos, varias tareas, proyectos, libros de texto, investigación, y evaluaciones.

- Entiendo que el Chromebook es solo para actividades escolares. El Chromebook no es para el uso personal.
- Entiendo que me debo encargar del cuidado de este Chromebook y protegerlo contra daño y pérdida
- Entiendo que no se permite instalar aplicaciones no aprobadas en el Chromebook.
- Entiendo que el mal uso del Chromebook puede resultar en la pérdida del privilegio del uso del Chromebook en la escuela.
- Entiendo que hay que cumplir con todas las reglas y espectativas del uso de tecnología de St. Helena.
- Entiendo que el Chromebook es la propiedad de St. Helena y que la escuela mantiene el control y supervisión del Chromebook, las redes y servicios internet de la escuela, y todas actividades hechas por el internet de la escuela/en los Chromebooks de la escuela. La escuela tiene el derecho supervisar el uso de intenet por los alumnos. Yo, como un alumno, no tengo ninguna espectativa de privacidad en mi uso de los Chromebooks de la escuela, incluyendo correos electrónicos y datos guardados en el Chromebook, y actividad en el internet.

Evitar Riesgos y Peligros Potenciales

El robo de identidad, ataques phishing, y estafas con temas comúnes y conocidos. Para evitarlos, se recomienda:

- No publicar datos personales en el internet. Hasta publicar fotos en grupos o perfiles no exclusivos a conocidos puede traer riesgos. Las fotos pueden indicar donde uno estaba, el momento cuando una foto fue sacada y otra información personal. Existe el riesgo que algiuen use esta información para victimizar a otro.
- Visitar exclusivamente sitios recomendados por los padres/apoderados o profesores. Se recomienda preguntar si un alumno tiene dudas sobre un sitio.
- Enfocarse y leer todo en un sitio no conocido y en correos electrónicos mandados por desconocidos. Si algo en el sitio no tiene sentido, si parece demasiado bueno para ser verdadero, o si parece faltar detalles o calidad en su presentación, uno tiene buena razón por dudar la seguridad del sitio.
- No responder a nada que requiere acción inmediata, como hacer click en un enlace sugerido, sin consultar a un adulto.
- Antes de ingresar datos personales, incluyendo datos de ingreso, asegurar que la dirección URL esté correcto. Es posible hacer click en enlace para un sitio, servicio, o negocio de confianza y entrar a un sitio falso muy parecido al verdadero. Para revisar la dirección URL en un computador MAC, se hace click en el espacio de direcciones donde hay una pequeña imagen de un candado o las letras ‘’https://’’.
- Recordarse: No requiere mucha información para identificar a una persona. Se puede identificar a la gran parte de personas con solamente tres datos: género, fecha de nacimiento, y código postal.

Artículos pertinentes (en inglés)

Risks on the Internet. Massachusetts Institute of Technology, https://ist.mit.edu/security/internet 23 Aug. 2016.
How to recognize a fake URL. eHow.com. http://www.ehow.com/how_2003266_recognize-fake-url.html 23 Aug. 2016.

Firma del Alumno _____ Fecha _____

He leído y acepto las responsabilidades y reglas descritas en este acuerdo.