Coventry Public Schools
Go Guardian Protocol

GoGuardian, a service that provides Chromebook monitoring, filtering and theft recovery, is part of the overall digital network security system for Coventry Public Schools. This system works in conjunction with the Google Apps for Education digital learning ecosystem.

The Coventry Public Schools Google Apps for Education system allows for users to be grouped into organizational units (OU) according to their role in the district. The system is divided into Employee OU's and Student OU's. Student OU's are further separated into high school, middle school and elementary school so permissions can be set for each group based on age. Our security vendors are CIPA compliant.

DISTRICT LEVEL ACCESS AND SECURITY MANAGEMENT

DISTRICT ACCESS:
Go Guardian has two levels of access.
SuperAdmin Role: Access to all aspects of the GoGuardian system.

This access level is assigned to the following:

Director of Technology
Director of Educational Technology

This level of access is protected via a two-way, shared password. Each director will know part of the password. Both directors must be physically present to enter their portion of the password in order to access this level of GoGuardian. No one person will have the complete password.

Admin Role: Access to all aspects of the system EXCEPT Audit Logs and Theft Recovery as these are at the SuperAdmin level only.

This access level is assigned to:

District Network Administrator

(A Roles/Permissions diagram is provided at the end of this document.)

DISTRICT SECURITY MANAGEMENT:
FILTERING: Access: SuperAdmin and Admin level
Websites are blacklisted based on Go Guardian's CIPA compliant categories list and additional categories and keywords listed by the district. The system's proprietary content-based filtering software tracks and analyzes every website visited and flags sites that might contain questionable content thus allowing for further review of a site for possible addition to the blacklist.

MONITORING: Access: SuperAdmin and Admin level
To further protect students while online, Chromebook activity is monitored to determine how the devices are being used and what is being accessed during the school day. This information provides analytical data for Chromebook use, and provides specifics on flagged activity by individual users.

THEFT RECOVERY: Access: Super Admin level **only**
In the event a Chromebook is reported stolen, the theft recovery feature of GoGuardian will be utilized by the district. This feature provides advanced geolocation technology to pinpoint the location of the stolen Chromebook on a map for reporting purposes. In addition, this theft recovery feature provides screenshots, keylogs, and webcam snapshots from the stolen Chromebook for the purpose of identifying who is using the stolen device. In order to utilize this feature, a police report must be provided to district administration. Because of the sensitive nature of this feature, the following protocol will be utilized:

1. Upon receipt of a police report, the serial number of the stolen device will be removed from its current Google Console OU and placed in an OU called Theft Recovery that is strictly reserved for the theft recovery feature. This will be the only device (serial number) in the OU. This will be the responsibility of the district network administrator who manages OU's in the Google Console. The network administrator will notify the Director of Technology that a theft investigation is ready to commence.
2. As noted above, the Theft Recovery feature in Go Guardian is only accessible at the superadmin level. The Theft Recovery feature will be activated via a two-way, shared password. The Director of Technology and the Director of Educational Technology will each enter a portion of the password that is specific to them thus activating Theft Recovery on this specific OU. By activating this feature, the camera projection will only be visible on this single device located in the theft recovery OU. This feature shall only be activated when the two authorized individuals listed above are present.
3. Once activated, recorded activity will be documented on the Chromebook Theft recovery form, signed, and submitted to the Coventry police and the school administration.
4. After the investigation is completed, the network administrator will be notified and the device (serial number) will be transferred to an OU labeled "Reported Stolen" as this OU will disable all features of the Chromebook and lock it down.
5. Once the device is recovered, it will be submitted to the technology office for evaluation. If it is operable, it will be returned to its original OU and returned to its assigned student for use in school.

IMPORTANT NOTE: The Theft Recovery feature **is not automatically enabled** on all Chromebooks. It is exclusively used according to the protocol described above.

SCREEN SHARE: GO GUARDIAN FOR TEACHERS - DISTRICT SETUP
To assist teachers in managing a digital classroom and to ensure devices are utilized in the classroom for instructional purposes under the guidance of a teacher, GoGuardian For Teachers, a screen share feature, is enabled at the district level for all student devices only. To ensure teachers will have limited access to viewing student screens, this feature is configured according to the following parameters:

1. District IP
   In order for the screen to be visible, the device must be connected to the Internet via the district network IP.
2. Time
   The screen share feature will be enabled Monday through Friday from 7:30 am to 2:30pm.

SCREEN SHARE: GO GUARDIAN FOR TEACHERS - PROTOCOL FOR TEACHER USE

All teachers will be able to use GoGuardian For Teachers and monitor their students' online activity, lock student screens to specific websites, and refocus attention to online educational tasks while in the classroom.

Although screen share is available during school hours, teacher use is restricted to use with students assigned to them during a specific class period. Access to student screens beyond their assigned class with an individual teacher is not allowed.

Theft Recovery Protocol