GALLIPOLIS CITY SCHOOL DISTRICT

GENERAL NOTICE OF MONITORING OR ACCESSING STUDENT ACTIVITY ON SCHOOL-ISSUED DEVICES

Ohio Revised Code §3319.327

This notice is provided to meet requirements implemented through Ohio Senate Bill 29 ("SB29") that was passed by the Ohio General Assembly, effective on October 24, 2024.

While students have no right or expectation of privacy when using District technology resources, the Gallipolis City School District (also referred to as the "District") and certain third-party technology providers that provide services through a contract with the District are prohibited by State law from electronically accessing or monitoring certain features on school-issued devices provided to students unless a legally permissible exception exists. The prohibited features include location-tracking features of a school-issued device, audio or visual receiving, transmitting, or recording features of a school-issued device, and student interactions with a school-issued device including, but not limited to, keystrokes and web-browsing activity. School-issued devices are defined as any hardware, software, devices, or accounts that a school district provides to an individual student for that student's personal use.

The Gallipolis City School District is required to annually provide parents and guardians with this general notice that informs you, the District, and its technology providers of the plans to electronically access or monitor your student's school-issued devices for the following permissible reasons:

- Activity that is limited to non-commercial educational purposes for instruction, technical support, or exam proctoring by School District employees or staff contracted by the District. Teachers may monitor students as they work on assignments during class to ensure they are staying on task.

- Pursuant to a judicial warrant. The District is required to comply with a lawfully issued warrant that directs the District, technology providers, or law enforcement to conduct a search of data.

- Notification or awareness that the student-issued District device is lost or stolen. This might occur if the District becomes aware that a student's device is lost or stolen, in which case the District or technology provider might access and monitor data to discover when and where the device last interacted with the District's systems.

- Activity is necessary to respond to a threat to life or safety. The access is limited to this purpose alone. For instance, the District may receive alerts about possible self-harm indicators on student devices that prompt an investigation which involves accessing or monitoring student data. The District implements other protocols such as contacting parents/guardians and/or first responders.

- Compliance with Federal and/or State laws. The District may be required to comply with a law that places an obligation on the District to access or monitor devices.

- Required as part of a Federal or State funding program. For example, to comply with the requirements of the Federal E-Rate funding programs, the District filters all student Internet access pursuant to the Children's Internet Protection Act. This includes filtering materials that are obscene, objectionable, inappropriate, and/or harmful to minors.

This electronic monitoring can only occur when advance notice is provided. No further notice is required for the District to monitor under reason #1. In the event that one of the circumstances listed in reasons #2-#6 occurs, the District will provide you with a seventy-two (72) hour notice of what features of the device were accessed, a written description of the circumstance, and description of the threat, if any. If the notice itself could pose a threat to life or safety, the seventy-two (72) hour notice will be provided within seventy-two (72) hours after the threat has ended.

Sincerely,

Craig Wright
Superintendent