General Notice of Monitoring or Accessing Student Activity on School Issued-Devices

Date: July 29, 2025

The District recognizes and appreciates the importance of parents understanding how the District protects students' privacy against unauthorized access while using school technology, as well as the circumstances in which the District may access or monitor certain student activity.

The Jackson-Milton Local School District (also referred to as "District") and certain third-party technology providers that offer services through a contract with the District are prohibited by Ohio law from electronically accessing or monitoring certain features on school-issued devices provided to students unless legally permissible exceptions exist (listed below). The prohibited features include location-tracking features on 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 history. 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 Jackson-Milton Local School District is required to annually provide parents and guardians with this general notice that informs you, the District, and technology providers of the plans to electronically access or monitor your student's school-issued devices for the following permissible reasons:

1. 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 on-task behaviors.
2. Pursuant to a judicial warrant. The District is legally obligated to comply with a lawfully issued warrant that directs the District, technology providers, or law enforcement to search data.
3. 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.
4. Activity is necessary to respond to a threat to life or safety. 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 that involves accessing or monitoring student data. The District implements other protocols, such as contacting parents/guardians and/or first responders.
5. Compliance with Federal and/or State laws. The District may be required to comply with a law that obligates the District to access or monitor devices.
6. 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 of #2-#6, the District will provide the parent/guardian with a notice of the features of the device that were accessed, a written description of the circumstance, and a description of the threat, if any. If the notice itself may pose a threat to life or safety, the notice will be provided after the threat has ended.

Sincerely,
Kirk Baker
Superintendent

Note: This notice is provided to meet the requirements of Ohio Senate Bill 29 (SB29) that was passed by the Ohio General Assembly, effective October 24, 2024.