

Why Kite Student Portal Requires Location Access on Windows 11

To ensure the reliable operation of the Kite® Student Portal on Windows 11, global location access must be enabled at the operating system level. This requirement stems from the way Windows 11 handles system-level geolocation APIs and their interaction with security-restricted or sandboxed environments like Kite Student Portal.

We recognize that privacy is a critical concern, and we want to be fully transparent about this setting. The Kite team is committed to safeguarding user privacy in every environment where our application is deployed. This notice is part of our proactive effort to keep you informed and help ensure a seamless testing experience.

Important Privacy Notes

- Kite Student Portal does not access, collect, or use physical location data.
- Enabling location services allows Windows to operate properly; it does not grant our app access to your location data.
- This setting supports essential OS functionality required for secure and stable application initialization.

Additional Context from Microsoft

- Location services are entirely user-controlled; you can toggle them on or off at any time.
- Manage location services access globally or on a per-app basis.
- Some Windows features depend on location services being enabled, even when no app is actively using your location (e.g., time zone settings or secure service initialization).
- Microsoft includes numerous built-in privacy protections, even when location services are turned on, such as:
 - The ability to manage which apps have location access.
 - Options to view or clear the device's location history.
 - Location data handling in accordance with Microsoft's published privacy policies.

For additional details, please visit Microsoft's [Windows Location Service and Privacy](#) page.

