



July 2026

Dear Parents and Partners,

We are writing to update you on how students connect to the internet at school, and to ask for your support in ensuring everyone stays connected and safe.

To comply with UK safeguarding laws, the school is required to block harmful content (such as adult material or gambling sites) on our Wi-Fi. To do this, we have an advanced filtering system called **Securly**, this filtering system requires users to install a certificate on their devices to allow us to ensure we can keep them safe online and identify any worrying behaviour.

1. Installing the Safety Certificate

To join the school Wi-Fi, every student must install a small file (a "certificate") on their phone or laptop. This tells our system that the device is authorized to use our network. This certificate is only active when the device is connected to our network.

2. Privacy (What we see vs. What we don't)

We know privacy is important. We want to be clear:

- **We DO** block access to unsafe or illegal websites and investigate alarming activity.
- **We DO NOT** read private messages or spy on personal data. We cannot see inside apps like WhatsApp, WeChat, or iMessage, and we cannot see private banking information.

3. VPNs and Private Relays

Apps that hide web traffic (VPNs) will stop the school Wi-Fi from working. If a student is using a VPN, the Wi-Fi will not work. They will need to switch these off to be allowed onto our network, additionally if parental controls are enabled this will also stop the Securly system from working.

How we are helping

Our IT department is currently visiting the boarding houses to help students set up their devices personally.

We would appreciate your help in reassuring students that these steps are standard for UK schools and are there for their safety.

With thanks and all best wishes,

Tony Oulton
Headmaster

