

Technical and Data FAQs

Who are Blackout?

Blackout is a UK-based company working remotely across the country, primarily from London and Bristol. We develop, maintain and support Blackout as our sole product, which is used across schools, workplaces and fleet environments.

Does Blackout track my child's location?

No. Although the app supports location services for other sectors (such as workplace and fleet customers), schools do not use this functionality.

Location permissions are disabled by feature flags and are never requested in a school environment.

Why does the app include location permissions?

Blackout is a single app used across several industries. Some workplace and fleet customers use optional location-based features, so these permissions must exist within the app. They are **disabled for schools**.

Can Blackout see which apps are installed?

No. App usage information remains private and is not collected or stored by Blackout.

On Android, Blackout briefly checks which app has been opened to determine whether it should display the blocking screen.

On Apple, Blackout uses Apple's Screen Time framework, which automatically provides the app name that appears on the blocking screen when a blocked app is launched.

What data is needed to set up Blackout?

For schools, Blackout collects minimal data to set up the app.

This includes:

- Student name
- School email address
- Year group / Form group
- Device type

Blackout **cannot** see photos, messages, browsing history, installed apps, websites visited, social media activity nor app content.

What operational data is collected?

- App version
- Battery level
- Permission status
- Whether the device is blocked, disabled or has not checked in recently

The system does record the number of times a student attempts to access blocked apps during school hours. This is used for reporting and analytics rather than monitoring content.

Where is data stored?

Student data is stored within the European Economic Area.

Primary systems include:

- AWS Dublin (EU-West-1)
- Google BigQuery EU region (for anonymised analytics)

Some operational services, such as Firebase notifications, may involve Google's global infrastructure, including the United States, using approved GDPR safeguards.

Technical and Data FAQs

Is data encrypted?

Yes - all data is encrypted:

- in transit
- at rest
- in backups

Blackout also uses:

- Role-based access controls
- Two-factor authentication where required
- Single Sign-On (SSO)
- Audit logging
- Incident response procedures
- Regular external penetration testing

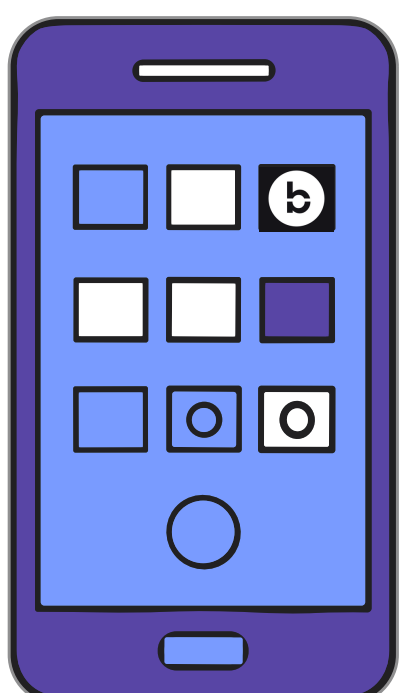
Does Blackout hold any security certifications?

Blackout does not currently hold formal certifications such as ISO 27001. However, the platform undergoes regular third-party security assessments and penetration testing, and work towards ISO 27001 is ongoing.

How long is data kept?

Data is retained only for as long as necessary. Operational logs and temporary records are generally deleted automatically after 90 days.

Full retention details are available within the Privacy Policy.



Which devices are compatible?

Blackout supports:

- iPhone: iOS 16 or later (iPhone 8 onwards)
- Android: Android 11 or later

Most modern smartphones are fully compatible. If a device is too old to support Blackout, the school may choose an alternative arrangement.

Has a Data Protection Impact Assessment (DPIA) been completed?

Schools are responsible for completing their own DPIA where required. Blackout provides documentation, including Data Processing Agreements and technical information, to support schools in this process.

Can parents request deletion of their child's data?

Yes. As the school is the Data Controller, requests relating to personal data should normally be made to the school, who will work with Blackout where appropriate.

Is Blackout safe for my child's phone?

Yes. Blackout is distributed through the Apple App Store and Google Play Store and uses only approved operating system APIs. Apps on both iOS and Android run within secure sandboxed environments, meaning Blackout cannot damage hardware or modify the operating system.

Technical and Data FAQs

Why does Blackout use a VPN?

VPN is used as an extra layer of protection to overcome any workarounds on Apple devices. This is only active during blocking periods.

The VPN:

- Does not monitor, report on, or store your internet activity.
- Is not a commercial VPN and does not provide anonymity or change your location.
- Only checks where traffic is headed so it can allow essential services (such as Blackout, Apple, and Safe365) and block everything else during scheduled blocking periods.

On iPhones, traffic passes through Blackout's servers while the VPN is active because this is how Apple's VPN framework works. There is very little data flow through this function. On Android, all filtering happens directly on the device.

Outside scheduled blocking periods, Blackout is not actively restricting your device.

