



Purpose

This statement clarifies how safeguarding and alerting responsibilities are shared between Senso.cloud and the Customer. It is especially relevant for schools, trusts and child safety use cases.

Platform role

- Senso.cloud provides tools and features that may generate alerts or notifications concerning activity through Managed Devices, depending on selected modules and configuration.
- The selected safeguarding, monitoring and filtering features are those stated in the accepted Order Form and enabled/configured by the Customer.
- Senso.cloud supports customer safeguarding workflows but does not replace professional safeguarding judgement, statutory duties or school policies.

Customer role

- The Customer is responsible for configuring safeguarding policies, alert thresholds, access roles, escalation workflows and review processes.
- The Customer is responsible for reviewing alerts, assessing context, deciding whether to act, and recording actions in accordance with its safeguarding and legal obligations.
- The Customer must ensure required notices, lawful bases and permissions are in place for monitoring and safeguarding activities.

Senso access to alerts

The Senso Terms state that Renato does not review Alerts or take action based on Alerts except as expressly authorised by the Customer. Any customer-authorised support access to the portal is just-in-time, logged and audited, and revoked after the engagement.

Optional integrations

Where the Customer opts in to third-party integrations such as Google Classroom, Microsoft Teams, Assisted Monitoring Services, MyConcern or CPOMS, those providers may receive access to relevant data as consented to and configured by the Customer.

Source basis

- Senso Terms of Service and End User Licence Agreement, Revised Oct 2023 V7, <https://senso.cloud/eula/>
- Senso Security Datasheet, revised 17 June 2024
- Supplier Data Security Assessment Questionnaire, completed 10 May 2023