

Parent Guide

Working Together to Keep Your Child Safe Online

Schools are legally required to protect children from harm, both offline and online.

They are expected to ensure that school managed devices and networks are safe, well-supervised, and able to detect early signs of risk. This includes having effective filtering and monitoring in place so that students' online activity is protected and staff are alerted to concerning patterns such as harmful searches, changes in behaviour, or exposure to inappropriate content.

Who Sets the Rules

Schools do not set online safety requirements on their own. They follow national child-safety expectations and standards set by key organisations responsible for protecting children online.



✓ Australian Government - eSafety Commissioner

Leads Australia's national online-safety framework, enforces the Online Safety Act, oversees the new under-16 social media restrictions, and provides reporting pathways for cyberbullying, harmful content, and image-based abuse.

✓ Australian Curriculum, Assessment & Reporting Authority (ACARA)

Integrates digital-safety and wellbeing expectations into the Australian Curriculum, ensuring students learn how to navigate online environments safely.

✓ State & Territory Education Departments

Set mandatory policies for safe technology use in government schools, including requirements for filtering, monitoring, device management, and childsafe standards

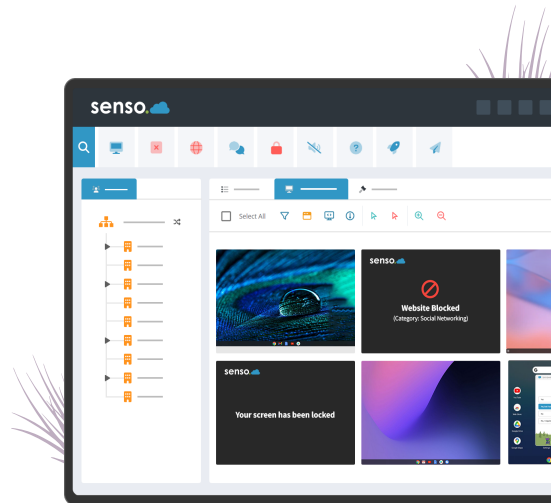
These organisations work together to ensure schools keep children safe when using digital technology, and Senso supports schools by providing tools to help them meet those obligations.

Who are Senso.cloud

Senso.cloud provides online safety, monitoring and classroom management tools used by over 10,000 schools worldwide. Our products are designed to support teachers with learning in the classroom and to help safeguarding teams meet their legal duties to protect children online, as required by Keeping Children Safe in Education (KCSIE).

All Senso products are developed in line with strict national guidance, including GDPR, Keeping Children Safe in Education (KCSIE), and the UK Safer Internet Centre (UKSIC) standards.

Our filtering tools have been officially approved by UKSIC's strict criteria required to block all illegal content. We do this by integrating the Internet Watch Foundation's URL list and the Home Office's CTIRU terrorist content list which ensures that harmful material such as child abuse imagery and extremist content is effectively filtered.



“Schools choose us because we follow strict guidance to create a safer, more controlled and more supportive digital learning environment for children.”

What does Senso.cloud do on your child's school device?

Senso.cloud's software supports your child's safety and learning in three key ways:

✓ Classroom Management

Helps teachers guide lessons and keep students focused. Tools allow them to manage screens, reduce distractions and support positive learning behaviours.

✓ Web Filtering

Works like a safety barrier on school devices. It helps protect children from harmful or inappropriate content by:

- Blocking unsafe or illegal websites (e.g. violence, pornography, extremist material).
- Limiting harmful searches (e.g. adult content, drugs, hate content).
- Ensuring online activity during school hours (and at home if school-owned devices are sent home) remain safe and appropriate.

✓ Safeguarding Monitoring

This adds an extra layer of protection. Using keyword detection, it captures keyword activity and patterns, only raising an alert if a word, phrase or pattern suggests a possible 'risk' to a child's safety or wellbeing based on our extensive keyword libraries. This helps safeguarding staff respond early and provide the right support to children.



What does Senso NOT do?

Senso.cloud is designed to protect children, **not to watch them**.

We do not:

- ✓ Spy on children.
- ✓ Record everything they type.
- ✓ Use webcams or microphones.
- ✓ Monitor personal or family-owned devices (unless the family has opted into the Bring Your Own Device (BYOD) scheme with their school).

“Our purpose is protection, not surveillance”.

Why might your child feel worried about monitoring?

Children sometimes misunderstand what monitoring means and think someone is “watching” them all the time.

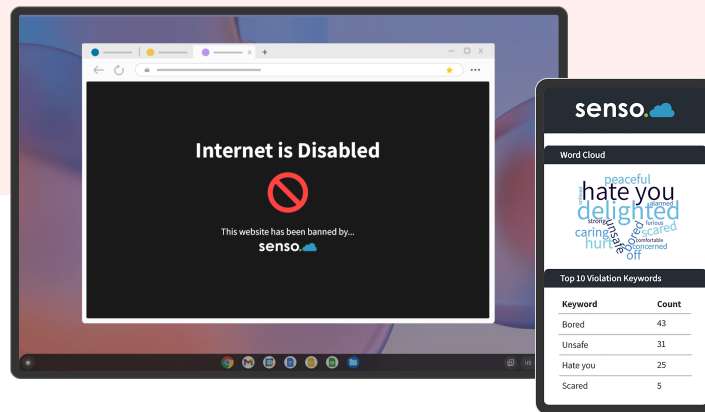
You can reassure them that:

- ✓ Monitoring only works on **school devices** (or those opted in to the Bring Your Own Device (BYOD) scheme).
- ✓ It can only see their personal messages if **typed on a school device** and **triggers a keyword** eg. On Teams or Google Chat.
- ✓ It only flags activity linked to **possible risk**, to try and keep children safe from harm.
- ✓ It is there to help **keep children safe** and support responsible online behaviours.
- ✓ Teachers and safeguarding staff use it to **support**, not punish.

Helping children understand this often reduces anxiety and makes them feel more secure.

What happens if something concerning is detected?

Depending on the school's configuration and set up choices, the safeguarding team in school will receive alerts based on severity and all captures will be logged for review within their portal.



How does Senso protect your child's privacy and data?

Senso.cloud is designed to help keep children safe while protecting their privacy. It only processes information that a school instructs it to process as part of its safeguarding and online-safety responsibilities.

Senso:

- ✔ Only monitors activity that relates to safeguarding risks.
- ✔ Only works on school-owned, school-managed or BYOD if opted in.
- ✔ Stores data securely in Microsoft Azure under strong security measures.
- ✔ Gives access to data only to authorised school staff, controlled by role-based permissions.
- ✔ Never uses cameras, microphones or personal device data.



The **school remains the data controller**, and Senso **processes information** on their behalf.

“Safety and privacy are built into our system at every level.”

For full details, you should refer to the school's own privacy notice, which explains how pupil data is managed by the school as data controller.