



# Technology Audit Checklist

---

Is your infrastructure supporting  
early intervention?



# Overview Technology Audit Checklist

Use this audit to challenge assumptions and stretch your school's digital infrastructure to better support early intervention, safety, and student wellbeing.

Whether or not you currently use monitoring tools, **these questions can help identify opportunities to strengthen visibility and response.**

## Technology Audit Checklist

### 1. Can your systems distinguish between curiosity, risk, and distress?

As online behaviours grow more complex, the ability to interpret context, not just content, is key to early intervention.

**2. Do your technology tools and vendors regularly update alerts to reflect emerging online behaviours?**

It is important to check with providers that your filtering or monitoring is set up to include encompassing new trends such as AI chatbot dependency, nudifying tools, anonymous Q&A platforms, or coded language.

**3. Who reviews digital incidents or concerns, and can they act on them?**

If incidents are routed to IT or a single wellbeing lead, is the capacity there to respond quickly? Could this be shared more widely across pastoral, leadership, or classroom staff?

**4. Do staff have visibility into patterns, not just one-off events?**

Do you have any systems or processes to track trends across year groups, time of day, or recurring search behaviours? What might be going unnoticed without that lens?

**5. Are digital behaviours connected to pastoral or academic data?**

How easily can you bring together signs from different areas, like changes in engagement, friendships, or classroom behaviour, to see the fuller picture?

**6. Are insights from online life feeding into support planning?**

Whether it's 1:1 meetings, escalation decisions or referrals, are digital behaviours part of that picture? Or do they sit outside pastoral systems?

**7. Is your filtering age-appropriate and educational?**

Are you creating learning moments by balancing protection with opportunities for digital responsibility — or shutting down access altogether?

**8. Do parents understand what your systems can and cannot do?**

Have you communicated the scope and limitations of your school's approach to online safety? Clarity reduces assumptions and increases community confidence.

**9. Can students speak up digitally and safely?**

Do students have confidential ways to raise concerns — whether via wellbeing check-ins, speak-up tools, or surveys? Early disclosures often happen away from adults.

**10. Is digital wellbeing part of your school culture, or just your tech stack?**

Do staff and students talk about online life openly and constructively? Or is it something that only gets discussed when there's a breach?