



Acceptable Use Policy

Clarity for Education

Version 1.1

Reviewed: 11 July 2026

Current external policy



Document control	Detail
Version	1.1
Reviewed	11 July 2026
Publication status	Current external policy
Review trigger	A material service, legal or safeguarding change, and at least annually

Purpose and status

This Acceptable Use Policy sets the rules for schools, trusts and authorised users of the Student Radar platform. It forms part of the service terms between SENDlink LTD, trading as Student Radar, and the customer.

The executed Order Form and Master Services Agreement govern the service supplied to a customer. If this policy conflicts with an executed agreement, that agreement takes priority.

Who this policy applies to

This policy applies to every person the customer authorises to access Student Radar, including school and trust leaders, administrative staff, teachers, SENCos, Designated Safeguarding Leads and other approved professionals.

The customer is responsible for assigning access appropriately, keeping authorised-user information current and ensuring its users understand this policy and the school's own safeguarding, information-governance and acceptable-use requirements.

Responsible and lawful use

Authorised users must:

- use Student Radar only for legitimate education, safeguarding, operational and pupil-support purposes within their role;
- follow applicable law, statutory guidance and the customer's policies;
- check that records are accurate, relevant and expressed professionally;
- use the minimum personal data needed for the task;
- respect confidentiality, intellectual-property rights and the rights of pupils, families and staff; and
- apply professional judgement to every action or decision supported by the platform.

Student Radar must not be used to harass, discriminate, mislead, facilitate unlawful activity or place a child or other person at risk.

Accounts and access

Each authorised user must use their own account. Users must not share credentials, allow another person to act through their account or attempt to use a role or permission they have not been assigned.

Users must:



- follow the authentication controls presented by the platform, including multi-factor authentication where required;
- keep passwords, recovery methods and devices secure;
- sign out of shared or unattended devices;
- report suspected credential compromise promptly; and
- stop using access that is no longer needed for their role.

Customers must remove or amend access promptly when a user leaves, changes role or no longer has a legitimate need.

Safeguarding and sensitive records

Student Radar supports recording and coordination; it does not replace the professional judgement or statutory responsibilities of the school, DSL, headteacher, governing body, local authority, police or children's social care.

Users must not:

- conceal, alter or delete safeguarding information without appropriate authority and a defensible record of the action;
- use Student Radar to avoid a required safeguarding referral, escalation or local procedure;
- disclose SEND, health, safeguarding or other confidential records to an unauthorised person;
- enter unnecessary third-party or case information; or
- use a public Student Radar tool as an official safeguarding reporting channel.

The school remains responsible for its safeguarding decisions, record quality, referral routes and retention instructions.

AI-assisted features

AI-assisted capabilities are advisory tools. An authorised professional must review the source information and output before relying on it. An AI output must not be the sole basis for a decision with legal or similarly significant effects on a pupil, and must not be treated as a diagnosis, statutory assessment, legal opinion or safeguarding decision.

Users must:

- use only AI capabilities enabled and approved by their school;
- follow any capability-specific notice about permitted inputs;
- avoid entering information that is not necessary for the approved task;
- correct unsupported, inaccurate, discriminatory or unsafe output; and
- record the human decision rather than presenting an AI suggestion as the decision-maker.

The free public Echo and Sensory Profiler tools are separate from authenticated school workflows. Visitors must not enter names, contact details, safeguarding narratives or other identifying case information into a public tool.

Prohibited technical activity

Users must not, without Student Radar's written authorisation:

- probe, scan or test the service for vulnerabilities;
- bypass authentication, permissions, rate limits or security controls;



- scrape or extract data in bulk outside an approved export process;
- reverse engineer, decompile or attempt to obtain source code or credentials;
- introduce malware or harmful code;
- interfere with availability, integrity or another customer's use; or
- access, alter or disclose data outside their authorised school, trust or role.

Good-faith security reports should be sent to dpo@studentradar.com without including credentials, pupil records or exploit details in the first message. Student Radar will provide a safer route where needed.

Content and communications

Users must not upload or send content that is unlawful, threatening, discriminatory, defamatory, malicious or knowingly false. Communications must be proportionate to the intended recipient and must not contain unnecessary pupil, health, SEND or safeguarding information.

Where SMS or transactional email is used, the customer remains responsible for the recipient list, message content, lawful basis and any required opt-out or communication preference.

Monitoring, investigation and enforcement

Student Radar may process security, audit and operational records needed to protect the service, investigate suspected misuse, meet legal obligations and support the customer. Such review must be proportionate and handled under the applicable privacy and data-processing terms.

Where reasonably necessary, Student Radar may restrict an account, function or item of content to contain a security or misuse risk. Urgent action may be taken without advance notice. Where circumstances allow, Student Radar will explain the issue and give the customer a reasonable opportunity to respond or remedy it.

Student Radar will not delete a customer's statutory safeguarding record merely because its content is disputed. Record correction, restriction, export and deletion must follow the customer's instructions, applicable law and the executed agreement.

Reporting concerns

Report suspected misuse, unauthorised access, data loss or a security concern promptly to dpo@studentradar.com. For ordinary product support, use support@studentradar.com.

Do not send passwords, API keys, pupil records or safeguarding case narratives through an unsecured initial email.

Changes to this policy

Student Radar may update this policy to reflect changes in the service, law, guidance or identified risk. Material changes affecting a customer's use will be communicated through an appropriate customer channel. An update does not override an executed agreement retrospectively.