

Security-Minded Communications: A Briefing for Schools

A school is open and welcoming by design. The catch is that the same openness which reassures parents can, without anyone meaning it to, hand a person planning harm a working map of your site. Security-Minded Communications is the free habit of checking what you publish before you publish it. This briefing is for anyone who runs your website, newsletters, social media or events.

The idea in one line

Think like the reader you do not want. Share what your real audience needs without gifting what a planner wants. It works two ways: **deny** them useful detail, and **deter** them by showing your school is alert and connected. Neither costs anything, and both apply to the channels you already use.

What someone planning harm is looking for

Specialists call the watching and information-gathering stage **hostile reconnaissance**. Someone at this stage wants to know: is this a suitable target, when is it busy or empty, what method would work, and where are the security gaps? They gather it online, from your website, Google Maps, Street View and social media photos, and in person, sometimes by simply asking staff, contractors, volunteers, parents or pupils.

Deny: habits before you publish

- Review what is already public, and what you are about to post, through a planner's eyes. This one honest check catches most of it.
- Keep the most detailed information in closed channels (a mailing list, private group or booking system); publish a lighter version openly.
- Avoid exact numbers. "Only 100 places" tells a watcher the size of the crowd.
- On maps and virtual tours, show public areas only. Leave out corridors, dimensions, and entrance and exit detail. Consider escorted-only visits.
- Use central school contact details in public materials, not named personal ones, which also help targeted phishing.
- Where you can, post about an event afterwards rather than trailing it in advance, especially with a high-profile guest.

Deter: what to say

- Promote the security you genuinely have, and only that. Inventing measures is worse than silence.
- Reassure, do not alarm. "Keep an eye out for anything out of the ordinary" beats "report suspicious people".
- Show your connections: a visit from a local officer or Safer Schools contact signals a wider network of vigilance.
- Be vague about when the site is empty. Posts across evenings and holidays suggest activity.
- Let staff be recognisable by a lanyard, but avoid showing pass detail clearly enough to copy.
- Make it obvious how to raise a concern, and that it will be taken seriously.

REPORTING A CONCERN

999 in an emergency **101** for non-emergencies Anti-Terrorist Hotline **0800 789 321**

Report online at gov.uk/ACT

FIVE-MINUTE SELF-CHECK

- ☐ We have looked at our website, social media and newsletters through the eyes of someone intending harm in the last year.
- ☐ Our maps and virtual tours show public areas only, without corridor, exit or dimension detail.
- ☐ Event posts avoid exact capacity and precise timings where they are not genuinely needed.
- ☐ Public materials use central school contact details, not personal ones.
- ☐ We promote only the security measures we actually have in place.
- ☐ Our safety language reassures rather than alarms.
- ☐ Staff and volunteers know what hostile reconnaissance is and how to report something that feels out of place.

Based on the National Protective Security Authority (NPSA) guidance "Security-Minded Communications: Guidance for Educational Settings" (Crown copyright, 2023). This is an original Fyrfly Systems summary to help schools apply that advice, not a reproduction; read the original at npsa.gov.uk. Security-Minded Communications is free and is not something we sell.