School Image Extortion - Action Plan

Immediate (0-2 hours):

- **Secure:** Preserve ALL digital evidence (messages, URLs, metadata). Isolate the device (if possible, without powering it off).
- **Report:** Immediately inform the Safeguarding Lead or Deputy and Headteacher / Principal and all IT staff.
- **Assess:** Briefly assess the threat and identify immediate safeguarding concerns.
- **Restrict:** Change ALL relevant passwords (social media, email, admin). Consider temporary takedown of affected accounts / websites.
- **Contact:** Inform the police (if child sexual abuse material (CSAM) or imminent harm is likely). Consult local authority safeguarding. Report to the platform.

Short-Term (2-48 hours):

- **Team:** Form a crisis management / critical incident team (Safeguarding Lead, Head, IT, comms).
- **Legal:** Consult legal counsel (data protection, privacy, communications, criminal offences).
- **Log:** Create a detailed incident log (actions, decisions, communications).
- **Identify:** Identify ALL affected individuals (students, staff).
- **Communicate:** Develop a communication plan (for staff, parents and students). Prepare scripted communication templates. Coordinate with authorities.
- **Support:** Provide immediate pastoral / counselling support (internal / external).

Medium-Term (1-2 weeks):

- **Review:** Review / update ALL relevant policies (safeguarding, social media, data protection).
- **Train:** Provide staff training (online safety, responsible social media use, image-based abuse response).
- **Educate:** Focus on student education (age-appropriate online safety, responsible use, consequences).
- **Inform:** Communicate with parents (online safety, support, resources).
- **Network:** Connect with other affected schools / networks for shared learning and support.

Long-Term (Ongoing):

- **Evaluate:** Regularly evaluate response effectiveness and policy updates.
- **Prevent:** Implement preventative measures (enhanced online safety education, appropriate monitoring).
- **Protect:** Strengthen data protection / security measures.
- **Engage:** Engage with the community (online safety awareness campaigns).

Your approach should always be:

- Child-centred.
- Trauma-informed.
- Confidential (respect privacy).
- Transparent (carefully balanced with protection).
- Collaborative (internal & external agencies).

 p 17.02.25 v1.0.1 www.ineqe.com