Safeguarding Bedfordshire: COM Group Briefing
March 2026

1. Purpose and Context

In October 2025, the National Crime Agency, working with the National Police Chiefs' Council (NPCC) and Counter Terrorism Policing, has issued an Early Threat Identification Notice specifically for safeguarding professionals. Its aim is to **raise awareness and enable early identification** of a serious emerging online threat called **'Com groups'** also referred to as 'COM Networks'.

This briefing summarises the notification and is designed to raise practitioner awareness. It is not for children, young people, parents, or carers.

2. What Are "Com Groups"?

- **Definition:** Online networks of individuals who collaborate or compete to cause serious harm across multiple criminal behaviours, often emerging and evolving rapidly.
- **Platforms:** They operate on commonly used **social media, messaging apps and online forums** frequented by young people, **not just on the dark web.**
- **Composition:** Membership varies but, in many cases, includes young male users who may seek **status, notoriety, power or control** by escalating the severity of harm they inflict or share.

Examples of harmful group behaviours include:

- Sharing **extreme and illicit content** (including violent, misogynistic and abusive material).
- Grooming or coercing victims, often **children or vulnerable individuals, into self-harm, violence or sexual acts.**
- Using **blackmail and extortion (including sextortion)** to obtain intimate images or compliance.

3. Nature of Harm

Com group activity may include:

- Grooming and coercion of children and vulnerable individuals; Targets are often approached through social interactions online, leading to gradual isolation and manipulation. Coercive pressure may begin with seemingly harmless requests then progress to demands for sexual content, self-harm or abuse of others.
- Sexual exploitation and image-based abuse (including sextortion). Intimate images are used to manipulate victims, sometimes involving threats of exposure to family or friends.
- Encouragement or coercion into self-harm or violence.
- Sharing of extreme, abusive or degrading material.
- Cybercrime and hacking activity.

A defining feature is **competition for status**, where perpetrators escalate harm to gain recognition within the group. In the most serious cases, victims have been pressured to record or livestream harmful acts.

4. Why This Matters

- **Hidden in plain sight:** Platforms used are often those already accessed daily by children and young people.

- **Rapid Escalation** Harm can escalate quickly, within hours of contact. Victims may not disclose involvement until significant psychological or physical harm has occurred. *(The Guardian, Jan 2026)*
- **Overlap With Other Threats** Com groups can intersect with other harms such as Cybercrime and hacking activity, Extremism and violent ideologies and/ or Sextortion and other forms of exploitation.
- **Multi-agency relevance:** Education, social care, policing, health and youth services all have a role in early identification and response.

5. Indicators Practitioners Should Recognise

Practitioners should consider Com group risk where there is:

- Sudden social withdrawal or marked behavioural change
- Secretive or excessive device use, multiple online accounts
- Exposure to or sharing of increasingly extreme content
- Signs of coercion, fear, or blackmail linked to online activity
- Unexplained self-harm behaviours or disclosures of online pressure
- Reports of online "dares," tasks, or demands escalating in severity

No single indicator confirms involvement but patterns should prompt safeguarding consideration.

6. Next Steps

- Treat any disclosure of coercion, self-harm directives or abuse linked to online contacts as a **safeguarding concern.** Follow your safeguarding policy.
- Record and share intelligence with organisational safeguarding leads, and the local Safeguarding Children Partnerships.
- Provide safe spaces for young people to discuss online experiences without fear of blame.
- Ensure staff and volunteers are briefed on how to respond appropriately to disclosures involving coercion and online exploitation.

Designated Safeguarding Leads should;

- *Brief staff on the nature of this threat*
- *Reinforce clear reporting pathways for online harm disclosures*
- *Integrate awareness into online safety and RSHE approaches (Education settings)*
- *Avoid victim-blaming language when responding to sextortion or coercion*

7. Key Messages

- **Com groups represent a dynamic and evolving online harm threat** that is not confined to niche or encrypted spaces.
- Safeguarding practitioners must be **alert to tell-tale indicators, respond early, and coordinate swiftly** across agencies.