GROOMING VIA SPOTIFY

Mechanisms, Tactics & Child Safety Implications

Child Focus — Policy Department

Internal Document — For Staff & Partner Organisations Only

Classification: CONFIDENTIAL

Introduction

Global prevalence data indicates that online grooming has reached the level of a public health emergency, with approximately 27% of children experiencing online solicitation at some point before the age of 18. Reports of online enticement have seen an explosive rise, with NCMEC documenting a 156% increase in 2025 alone, while UK data shows an 89% surge in grooming crimes over the last six years. A critical trend is the stark rejuvenation of victims; there is a dramatic increase in groomed children under the age of 10. Furthermore, the traditional gender gap is shifting: while girls remain primary targets for romanticized manipulation, boys now account for significant portions of solicitation cases, particularly regarding financial sexual extortion.

The technological landscape is evolving rapidly, with generative AI and deepfakes acting as force multipliers for exploitation. NCMEC recorded a staggering 1,325% increase in AI-related reports, often used to create synthetic abuse material to sustain cycles of blackmail. Perpetrators are increasingly exploiting "blind spots" like Spotify, utilizing the "Follow-Back" (IFB) culture to signal vulnerability and personal playlist art for visual profiling. To evade detection, offenders almost universally employ "off-platforming," moving interactions from public social media to encrypted private messaging apps like WhatsApp or Telegram. Emerging "cult communities" also use grooming tactics to push isolated children toward self-harm or violent extremism.

Evidence-based research now firmly links digital grooming to physical safety risks, specifically child disappearance. In 2025, European hotlines identified 92 cases where grooming was the direct catalyst for a child going missing. This "grooming-missing" continuum manifests in three ways: children being persuaded to run away by a groomer, children fleeing out of fear or shame due to extortion (fallout), and missing children becoming highly vulnerable to exploitation while isolated from support networks. These findings underscore that grooming is no longer a standalone digital issue but a precursor to severe physical and psychological trauma.

This document provides a detailed, evidence-based analysis of the mechanisms through which predators identify, select, and groom minor victims on Spotify. It covers the platform's structural vulnerabilities, the social behaviours of minors that inadvertently lower protective barriers, and the stepwise psychological process perpetrators follow — from initial contact to active coercion and blackmail.

KEY FINDING

Spotify's combination of public profiles, searchable usernames, playlist cover photos, and a direct messaging feature creates a functionally complete grooming environment that is rarely scrutinised by safeguarding professionals or parents.

1. How Minors Expose Themselves: The "Follow-Back" Culture

A recurring behaviour observed among younger Spotify users is the display of "IFB" (I Follow Back) in their profile name or bio. While the motivation is purely social — gaining followers to increase perceived status on the platform — this practice has significant and largely unrecognised safety implications.

Mechanism

The minor publicly signals that any account that follows them will be followed in return. The goal is to inflate follower counts and gain social credibility within peer networks. From a safeguarding perspective, however, this practice substantially lowers the barrier for unknown adults — including potential perpetrators — to establish an initial connection without triggering suspicion.

Risk Exposure

By broadcasting an unconditional follow-back policy, the child effectively invites the broader platform community, including strangers, to monitor their activity, access their playlists, and initiate contact. Perpetrators actively search for profiles bearing "IFB" designations precisely because these users are less likely to block or report an unfamiliar follower.

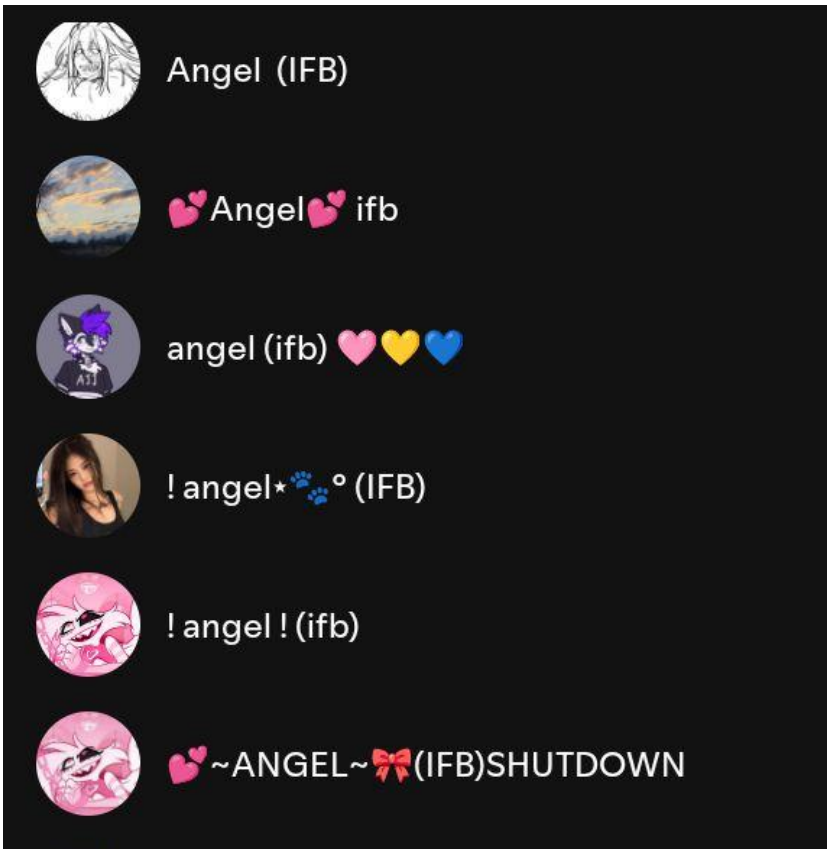


Figure 1 — Spotify profiles displaying "IFB" (I Follow Back) in the username, a common practice among younger users that inadvertently increases exposure to unknown contacts.

SAFEGUARDING IMPLICATION

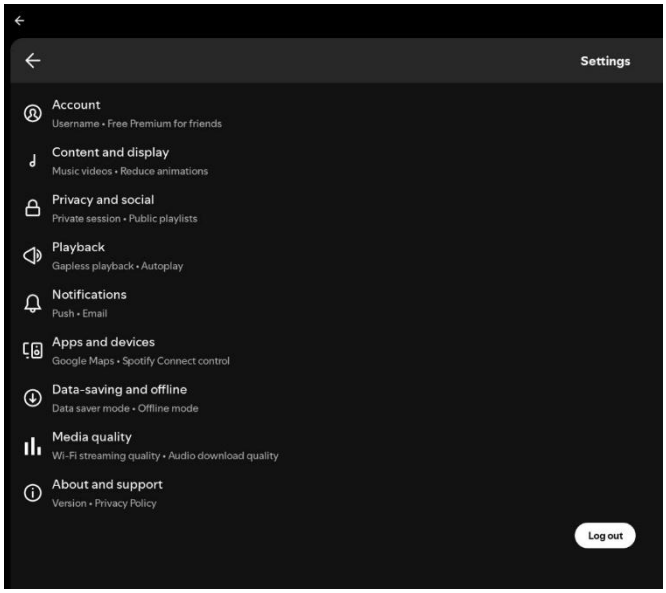
Children and parents are generally unaware that "IFB" functions as a visible vulnerability signal to potential perpetrators. Awareness campaigns should address this specific behaviour as a priority.

2. Platform Architecture as an Enabler: Privacy Settings

Beyond individual behaviour, Spotify's default and user-configurable privacy settings play a direct role in determining the level of exposure a minor's profile carries. When privacy restrictions are disabled — either by default or through deliberate (but often uninformed) user action — the profile becomes fully accessible to external parties.

The Risk of Open Privacy Settings

Spotify's Privacy and Social settings include controls over profile visibility, follower and following display, playlist visibility, and crucially, messaging. When a user disables these restrictions, they eliminate the primary technical barrier that would otherwise prevent unsolicited contact from outside their established social circle.



For a minor, this is rarely a deliberate choice to enable contact with strangers. More commonly, it results from a desire to participate in platform social features, or from a lack of awareness that these settings exist or carry risk. The outcome, however, is the same: the profile becomes functionally indistinguishable from an adult's open account and is equally accessible to perpetrators.

Figure 2 — Spotify's Privacy and Social settings panel. When profile visibility and messaging toggles are disabled, the account is open to contact from any platform user.

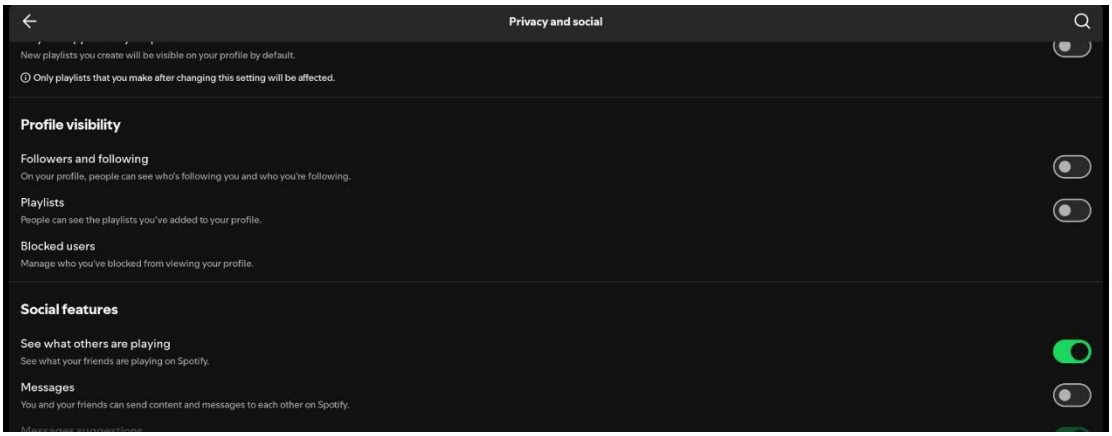


Figure 3 — Detail view of profile visibility and social feature toggles. Perpetrators look specifically for accounts where messaging and follower visibility are unrestricted.

POLICY NOTE

Spotify does not enforce age-differentiated privacy defaults. A 12-year-old's account carries the same default privacy architecture as an adult's. This represents a structural gap that warrants direct engagement with the platform through regulatory and policy channels.

3. Victim Selection: How Perpetrators Identify Minors

The process by which perpetrators select minor victims on Spotify is deliberate, structured, and leverages the platform's search and browsing functionality. It is not a passive process — it involves active scanning and visual analysis.

Observation and Targeting

Perpetrators use Spotify's profile search feature to browse user accounts. Profile photos are the primary selection criterion: users with photos that visually suggest youth are flagged as potential targets. This is compounded by bio content, playlist titles, and social signals such as IFB designations. Accounts that combine a youthful appearance with open privacy settings and an IFB profile are considered high-priority targets.

Initial Contact

Once a profile has been identified as belonging to a minor, the perpetrator initiates contact. The approach is typically non-threatening and framed around shared musical taste — commenting on playlists, following the account, or sending an initial message that references the child's listening activity. This creates an apparently legitimate reason for contact that is unlikely to raise immediate concern.

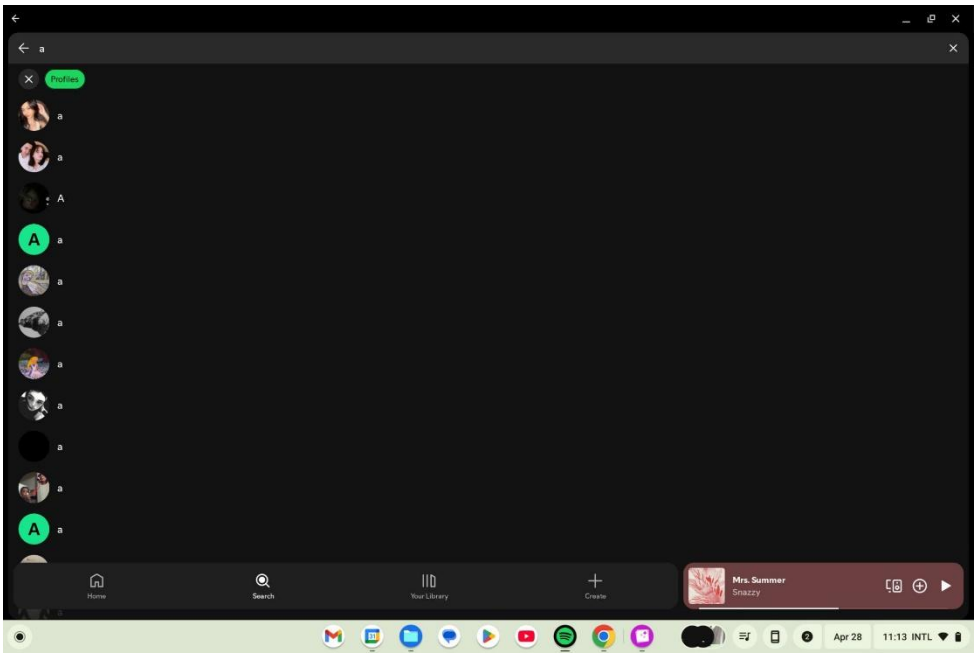
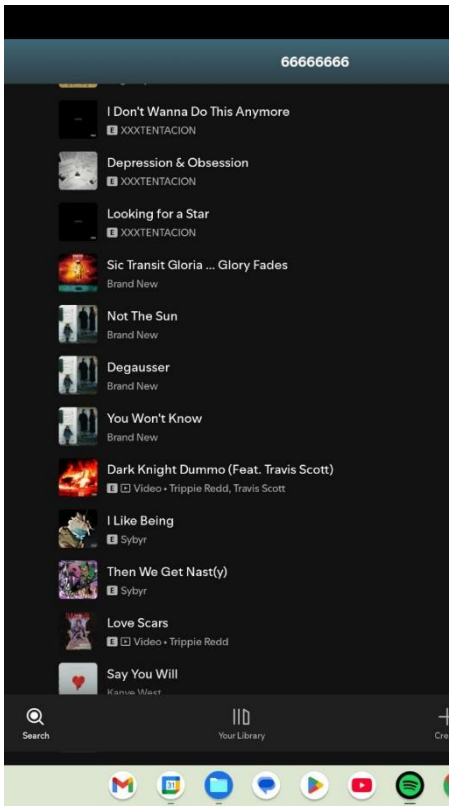


Figure 4 — Spotify's profile search results filtered by username. Perpetrators scroll through profile photo thumbnails to identify accounts belonging to minors.

4. The Social Valuation of Personal Data



A structural dynamic observed consistently in these cases is what can be described as the social valuation of personal data: the minor perceives a direct exchange between personal disclosure and social reward. The more a child shares — whether through personal photos, candid playlist covers, or detailed profile bios — the more followers, saves, and engagement their profile attracts. This creates a reinforcing loop in which privacy erosion is incentivised by the platform's social mechanics.

Mechanism and Risk

Children and adolescents, particularly those with lower self-esteem or a strong desire for peer validation, are especially susceptible to this dynamic. The playlist cover — often a personal photograph — becomes a social asset deployed to attract followers. From the perpetrator's perspective, these photographs are intelligence: they convey physical appearance, approximate age, family composition, and emotional state.

Figure 5 — A minor's playlist list, using personal photographs as cover art. These images provide perpetrators with visual intelligence about the child.

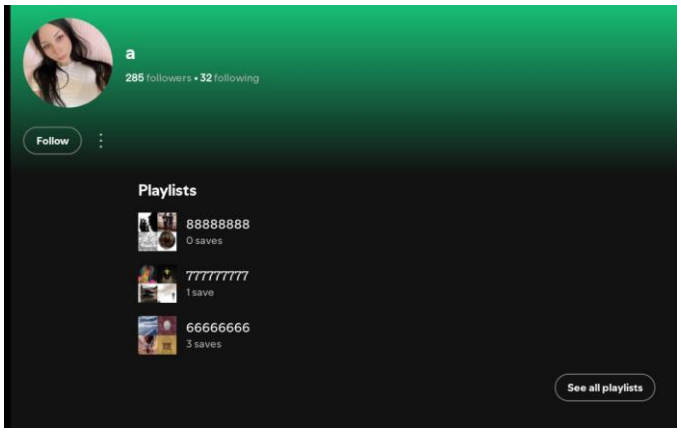


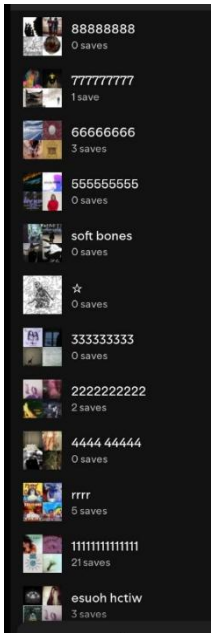
Figure 6 — Spotify profile showing follower count alongside public playlists. The platform's social architecture links visibility with quantified social status.

5. Visual Profiling and Family Analysis

Personal photographs used as playlist cover art serve a dual function in the grooming process. For the minor, they are a social tool. For the perpetrator, they are a resource for systematic visual profiling.

What Perpetrators Analyse

Photographs are examined for several categories of information:



- **Physical characteristics:** The physical appearance and approximate age of the primary subject
- **Siblings and family:** The presence of siblings, indicating the child's position within a family structure
- **Home environment:** Household environment details visible in background elements
- **Institutional identifiers:** School uniforms, sports kit, or other institutional affiliations that aid location inference

This analysis informs the grooming approach. Knowledge of a sibling, for instance, may later be used as a leverage point in coercive communications. Awareness of a school or neighbourhood allows a perpetrator to construct a plausible local persona.

Figure 7 — A publicly visible playlist library using personal photographs as cover art. The images collectively form a detailed visual record of the child's appearance and environment.

6. The Grooming Process: Psychological Conditioning and Coercion

The progression from initial contact to active exploitation follows a well-documented psychological trajectory. On Spotify, this process is adapted to the platform's social dynamics but follows patterns consistent with grooming across other digital environments.

6.1 Phase One: Trust Building (Engroomment)

Following initial contact — typically via Spotify's messaging feature, with subsequent migration to WhatsApp, Telegram or similar encrypted platforms — the perpetrator invests significant time in intensive, affirming communication. The goal is to establish emotional dependence and create the perception of an exclusive, understanding relationship.

The perpetrator deliberately positions themselves in contrast to the child's existing relationships: as someone who "truly listens" and "understands" in ways that parents, teachers, or peers do not. This is a

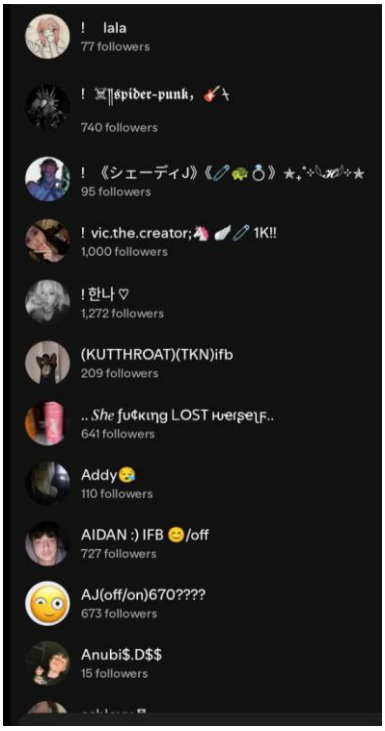
calculated strategy to isolate the child from their primary support network and establish the perpetrator as the most trusted figure in their social world.

Figure 8 — Example grooming messages: excessive affirmation, compliments, and declarations of affection intended to build rapid emotional dependence.

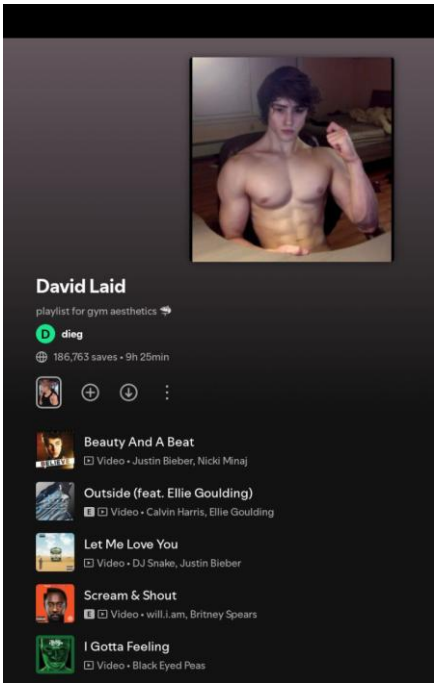
PATTERN TO RECOGNISE

Grooming conversations on Spotify typically begin with music-related topics, then shift rapidly to personal validation, compliments on appearance, and expressions of emotional closeness. The transition is often swift — within days of first contact.

6.2 Phase Two: Catfishing and Victim Profiling



Perpetrators routinely assume false identities (catfishing) to reduce the child's social guard. Fake personas are tailored to be maximally appealing and non-threatening to the target demographic: typically portraying someone slightly older than the child, attractive, and emotionally mature.



Target selection in this phase is not random. Perpetrators actively seek profiles that signal vulnerability: playlist titles or biographies expressing loneliness, low self-worth, family difficulties, or social isolation. These signals are interpreted as indicators of reduced adult supervision and heightened susceptibility to the validation the perpetrator offers.

Figure 9 — Profiles used in catfishing operations. Attractive, aspirational imagery is used to construct false identities designed to appeal to vulnerable minors.

Figure 10 — Follow network analysis showing the scale of victim targeting. A single perpetrator account may be following hundreds of minor profiles simultaneously.

6.3 Phase Three: Social Engineering and Network Infiltration

Having established trust, the perpetrator moves to map the child's social environment. Questions about crushes, close friends, and social conflicts are used to construct a detailed picture of the child's relationships and the social stakes associated with them.

This information is subsequently weaponised. The perpetrator creates an asymmetric knowledge relationship: they possess detailed knowledge of the child's world, while their own identity remains concealed. This asymmetry is the foundation on which coercive control is later built. The threat of exposing sensitive material to named individuals — friends, classmates, family members — generates disproportionate fear in adolescent victims due to the developmental salience of peer reputation.

6.4 Gender-Differentiated Manipulation Strategies

The literature and observed cases indicate distinct manipulation approaches tailored by perceived gender:

- **Approach targeting boys:** Misleading links (including location coordinates or video fragments) are used to appeal to curiosity or voyeurism. These function as an entry point to compromising the child digitally or physically.
- **Approach targeting girls:** The perpetrator first constructs a romantic relationship (charm phase). Once images have been obtained, the dynamic shifts to active sextortion, with threats centred on disclosure to school and family contacts.

These are patterns, not absolutes; the safeguarding response must not assume either approach is gender-exclusive.

7. Escalation Mechanisms and Advanced Coercion

7.1 "Empty" Playlists as Covert Exchange Channels

A technically notable tactic is the use of Spotify playlists as a channel for exchanging explicit material without audio content. Playlists are created using only metadata — titles and cover images — to communicate or transmit content. This exploits Spotify's content moderation blind spot: audio content is moderated; playlist metadata is not.

As the perpetrator accumulates material, demands escalate in a ratchet pattern: each image obtained is used as collateral to demand further, more explicit material. The child becomes progressively more entrapped, as the perpetrator's library of material grows and the threat of exposure becomes more credible.

7.2 Multi-Account Manipulation: The "Good Cop / Bad Cop" Dynamic

A sophisticated tactic documented in multiple cases involves the simultaneous deployment of multiple accounts against a single victim:

- **Account A:** Account A (the coercive actor) applies heavy psychological pressure, issues explicit threats, and creates acute distress.

- **Account B:** Account B (the "protective" figure) presents as a concerned friend or peer who offers sympathy, advises the child to block Account A, and positions itself as a source of safety and support.

Both accounts are operated by the same perpetrator. The effect is severe psychological disorientation: the child is simultaneously terrorised and offered comfort by the same individual, without any awareness that the two identities are connected. This completely neutralises the child's capacity to seek help from an authentic external source, as the only "safe" figure they trust is the perpetrator themselves.

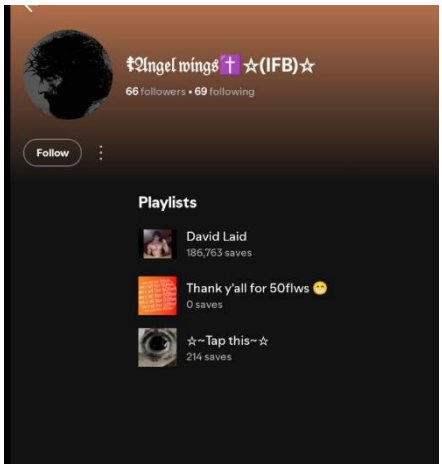


Figure 11 — Multiple Spotify accounts used in parallel against the same victim. The perpetrator controls both a threatening identity and a "supportive" one.

Figure 12 — Extended follower list showing a wide-scale targeting operation. The breadth of following activity indicates systematic, non-opportunistic predatory behaviour.

CLINICAL IMPLICATION

Children subjected to the Good Cop/Bad Cop dynamic frequently present as confused, unable to explain why they trust a contact they can simultaneously describe as frightening. Practitioners should treat this confusion as a red flag for multi-account manipulation rather than as inconsistency in the child's account.

8. Summary of Risk Indicators

The following indicators, observed across the victim profiles and case patterns described in this document, should be treated as safeguarding signals when identified in a child's Spotify activity:

- "IFB" (I Follow Back) in username or bio
- Personal photographs used as playlist cover art
- Privacy settings set to fully open (messaging enabled for all)
- Playlist titles expressing low self-esteem, isolation, or emotional distress
- Rapid acquisition of unfamiliar followers
- Evidence of contact with adult accounts not known to the child's social circle
- Playlists with no audio content (title/cover only) created in exchange with unknown contacts
- Disclosure of WhatsApp or other contact details in Spotify bio or messaging

9. Recommendations

For Child Focus and INSAFE/INHOPE Colleagues

- Develop platform-specific guidance on Spotify safety for inclusion in existing digital literacy programmes.
- Engage Spotify directly through regulatory and advocacy channels to advocate for age-differentiated default privacy settings and stronger messaging safeguards for under-18 accounts.
- Incorporate Spotify grooming patterns into professional training materials for law enforcement, social workers, and school counsellors.
- Publish parent-facing guidance that specifically addresses the IFB phenomenon and the safeguarding risks of personal photographs in playlist cover art.

For Frontline Practitioners

- When conducting digital safety assessments with minors, include Spotify in the review of social platform use alongside more commonly scrutinised platforms.
- Treat the Good Cop/Bad Cop confusion pattern as a diagnostic indicator rather than an inconsistency in the child's account.
- Be aware that grooming via Spotify typically migrates to WhatsApp, Telegram or similar messaging platforms within a short period; evidence may span multiple platforms.