

Moving Toward a Digital Future

A Roadmap for The Girls' Brigade
England & Wales



Contents

Executive Summary	3
Introduction & Context	4
The Girls' Brigade Now	7
Women and Girls in the Digital World	8
Comparative Learning	13
Recommendations for Safe and Effective Digital Youth Work	19
Preparing for Out-of-School Settings (OOSS) Requirements	35
Recommendations for Future Proofing Against OOSS Outcomes	37
Conclusion	39
List of Recommendations	40
References	47



Executive Summary

This report proposes a progressive and pragmatic strategy for The Girls' Brigade to develop and future-proof its work through the expansion of online youth provision, with a focus on holistic safeguarding integration. The goal of this work is to embed online youth work as a protective factor for young people, building upon The Girls' Brigade's existing strong culture and commitment to safeguarding as demonstrated in the *Life to the Full* policy.

The analysis identifies that while a strong safeguarding culture exists, there are areas that require attention to optimise its online delivery.

This report presents an assessment of the contemporary digital landscape, addressing critical issues facing girls and young women, such as AI-generated abuse, sextortion, grooming, and body image. Finally, it provides actionable recommendations designed to guide responsible digital activity, detailing how The Girls' Brigade can align its digital youth work with any of the Department for Education's proposed safeguarding approaches for Out-of-School settings, creating safe digital spaces that set a standard for the wider youth sector.

Done well, online youth work can itself be a protective factor. It can build digital resilience, nurture trusted relationships, and create safe spaces for support and belonging. The Girls' Brigade is well positioned to achieve this and is committed to ensuring safeguarding shapes every aspect of digital provision - from planning and training through to delivery and governance.



Introduction & Context



This report provides The Girls' Brigade with an evidence-informed assessment of how it can safely and effectively expand its youth work into online settings. It was commissioned in response to the growing preference for online engagement with young people. The report is not an audit of past performance. Instead, it offers a forward-looking, strategic exploration of what is required to future-proof the organisation's work, ensuring that safeguarding is embedded by design in any online youth engagement, consistent with The Girls' Brigade values and operational context.

Methodology

This report is founded upon a methodology that is multi-layered and evidence based. Both primary and secondary data has been collected to inform this report.

In the first instance, INEQE conducted thorough desktop research encompassing existing and proposed legislative changes, both of which are explored and placed within the context of The Girls' Brigade throughout this report. This research also included an extensive exploration of literature pertaining to safeguarding, youth work, online harms and violence against women and girls. A number of case studies have been analysed, and their detailed learning outcomes are included in this report.

Consultations were undertaken with a range of youth organisations engaging in online contexts with their children and young people. This included a comparative piece of work completed with The Girls' Brigade Australia. Leading experts within the field of safeguarding have also been consulted to inform the findings of this report.

Benchmarking

To ensure this report is grounded in recognised standards and sector expectations, the analysis was set against three key frameworks. These provide both a measure of where The Girls' Brigade stands now and a guide to what it will need to sustain safe and effective digital delivery in the future:

1. **National Youth Agency Digital Youth Work Standards (2025)** - providing a framework for good, great, and advanced digital practice.
2. **Working Together to Safeguard Children (2023)** - setting out statutory safeguarding guidance for all organisations working with children, including expectations around training, governance, and escalation.
3. **Out-of-School Settings (OOSS) consultation** - recognising the potential regulatory shift and preparing The Girls' Brigade to adapt and lead in this environment.

Why Online Youth Work and Safeguarding Must Be Considered Together

The Girls' Brigade has long recognised that safeguarding is not separate from youth work, but integral to it. That ethos is already evident across its face-to-face provision, where creating safe environments is central to the organisation's identity and culture.

As engagement moves into digital settings, the same principle applies. Online youth work creates new opportunities for connection and inclusion, particularly for young people who may be geographically isolated or otherwise excluded.

The risks young people face in the digital world, such as misogyny, image-based abuse, grooming, and harmful content, may already be part of their lived experience. By stepping into these spaces, The Girls' Brigade accepts both the opportunity to offer support and the responsibility to ensure that its online delivery is designed with safeguarding at its core.

The National Youth Agency (NYA) is clear that *'any youth work that involves the internet is online digital youth work'*. By that definition, The Girls' Brigade is already delivering elements of digital engagement through its communications, digital resources, and pilot sessions. The task now is not to start afresh, but to build on existing strengths and apply the same safeguarding first mindset to this next stage of delivery.





The Girls' Brigade Now

Organisational Ethos, Reach and Demographic

The Girls' Brigade is a Christian, volunteer-led organisation with a long-standing reputation for providing safe, inclusive, and values-driven youth work. With groups operating through local churches across England and Wales, The Girls' Brigade is distinct in its focus on girls and young women, with an ethos that combines faith, fun, and friendship. Its programmes are rooted in inclusion, with a strong emphasis on equality, diversity and inclusion (EDI). An independent assessment in 2024 recognised The Girls' Brigade's potential to become a 'trail blazer' in this field.

Current Practices and Pilots

While The Girls' Brigade previously focused on face-to-face delivery, they have already begun to test online engagement through pilot discussion groups with 14-18 year olds.

These sessions, covering topics such as Safe Night Out, Staying Safe in the Digital World, and Making Sustainable Choices, have demonstrated **three key points:**

- 1. An appetite among young people for meaningful online engagement.**
- 2. A commitment to co-design and co-delivery,** with young leaders and young people shaping both content and format.
- 3. An understanding that safeguarding measures must be built into sessions by having two leaders present,** chaplaincy support, parental consent, signposting to external agencies, and the option for participants to access breakout rooms for pastoral or safeguarding support.

Strengths to Build On

What is clear is that the organisation has both the culture and the commitment to adapt their existing safeguarding infrastructure to online environments.

Life to the Full functions as The Girls' Brigade policy 'bible', with addenda for online activity and supporting materials such as safeguarding flowcharts, risk assessments, and training resources.

Challenges Ahead

Adaptation to digital youth work will not be without challenges. The digital competence of volunteers is mixed, safeguarding materials are spread across multiple documents rather than consolidated, and local variation in practice can create inconsistency. These are not insurmountable obstacles - they are simply markers of where The Girls' Brigade's adaptability must now focus.

Women and Girls in the Digital World

// Research shows that over three quarters of girls aged 7-21 in the UK have experienced some form of online harm, ranging from unsolicited messages to image-based harm. //

Girlguiding, 2024

To protect and empower young people online, we must first understand the realities they face. For girls and young women, the online world is both a space of connection and creativity, but also one where harassment, coercion, and harmful cultures can be normalised. That said, safeguarding training across the sector is often underplayed or separates the online element, despite the fact that digital life is now inseparable from young people's lived experience. Unless organisations treat this as a safeguarding responsibility, they leave young people exposed.

The Girls' Brigade recognises this and is working hard to put the necessary safeguards in place. The Girls' Brigade's move into online youth work provides an opportunity to lead by example. By ensuring its staff and volunteers are fully equipped and knowledgeable in online safeguarding, The Girls' Brigade can set a standard for how youth organisations should adapt. Recommendations on how to strengthen this expertise will follow later in this report. For now, this section draws on national research to set out the digital landscape as it is experienced by girls and young women.

AI-generated sexual imagery

Artificial Intelligence (AI) technologies have made it alarmingly easy to create manipulated sexual images that are increasingly difficult to distinguish from those that are genuine ([IWF, 2025](#)). Globally, this poses profound safeguarding challenges. July 2024, in Spain, 15 male school children were prosecuted after creating and sharing AI-generated naked images of their classmates via WhatsApp. The court upheld convictions for creating child abuse imagery and required the boys to attend classes on gender equality and 'responsible use of technology', reflecting the severity of harm caused to the girls affected ([The Guardian, 2024](#)).

In other cases, images of girls have been taken from school websites or social media and manipulated using AI to create sexualised content. Such material has already been used to bully, blackmail, and exploit both students and staff (INEQE, 2025). Sadly, these incidents are not hypothetical. The reality is that they are happening now. Research shows that one in four young people have already encountered sexually explicit deepfakes online (Girlguiding, 2025).

'Self-generated' image abuse

Intimate image abuse remains one of the most prevalent online harms affecting girls and young women. The IWF (2024) has highlighted the growth of a so-called 'football card culture', where boys trade nude images of female peers, most frequently involving girls aged just 11-13.

National data reinforces the gendered nature of this abuse. The Revenge Porn⁴ Helpline (2024) reported that **on average, for every image of a man shared, approximately 24 images of women were distributed without consent.**

⁴ While 'Revenge Porn' is a widely recognised term, in INEQE's view, it risks minimising the seriousness of the behaviour by framing it as something less than abuse. We consider this to be more accurately understood as a form of online sexual abuse.

The Helpline also recorded that threats to share intimate images were the third most common issue reported. Perpetrators most often used private messaging apps, such as WhatsApp, Instagram and Snapchat, but in many cases also threatened to distribute images on highly public platforms, including adult pornography sites and social media.

While some young people may consensually share images in the context of relationships, many are pressured, coerced, or later victim-blamed when those images are misused. The combination of stigma and fear often leaves victims feeling isolated and prevents them from seeking support (Ray and Henry, 2024). When they do reach out, it is vital that the person they speak to has a nuanced understanding of consent and can offer appropriate pathways to support. Such an understanding recognises that consent must be informed and freely given, may be time-limited, and can be conditional or granted to a specific person under specific terms (e.g., that the image is not to be re-shared or kept beyond the bounds of a relationship).

Sextortion

In 2024, the IWF recorded a 2,600% increase in sextortion reports involving girls, with victims as young as 11 being targeted. In the first five months of that year alone, UK police received an average of 117 reports of sextortion from under-18s each month (NCA, 2025). The scale of the threat was so severe that the National Crime Agency issued its first ever nationwide safeguarding alert to schools, warning education leaders, staff, parents and carers about the risks.

Sextortion typically begins when perpetrators coerce or groom a young person into sharing a nude image. Once in possession of that image, they may demand further images, money, or exploit the victim through sustained blackmail. Motivations can vary. Some offenders seek financial gain, while others are driven by sexual gratification. Whatever the motive, the impact on victims can be devastating. Many describe feeling trapped, ashamed and fearful. With offences significantly underreported and with the crime often being misclassified under broader exploitation offences, the true scale is far greater than official figures suggest (Jurecic et al., 2016).



“Girls told us they don’t feel safe outside, at school, or online.”

Girls Attitudes Survey, 2023, p.8

The psychological consequences of this kind of extortion can be severe, leading to self-harm, and in some cases, suicide.

In a landmark case, Alexander McCartney became the first person in the UK to be convicted of manslaughter linked to sextortion ([PSNI, 2024](#)). Although the crimes themselves are sadly not unusual, the conviction marked a significant legal first and underlined the destructive consequences this form of abuse can have.

Grooming

In 2023-24, more than 7,000 offences of sexual communication with a child were recorded in the UK, with 81% of victims identified as girls ([NSPCC, 2024](#)).

Grooming often begins in public online spaces like gaming platforms or social media before shifting into encrypted apps such as WhatsApp or Telegram. Offenders may use ‘catfishing’⁵ to build trust, posing as peers or exploiting shared interests.

Victims often feel confused, ashamed, or fearful when manipulation is disguised as friendship or romance. Although girls often recognise these risks, they may not necessarily disclose abuse when it happens to them. *“Girls told us they don’t feel safe outside, at school, or online.”* – [Girls Attitudes Survey \(2023\)](#). In the McCartney case, police identified over 3,500 victims, yet only four came forward. Young people have explained this silence in terms of shame, embarrassment, and fear of how adults might respond.

⁵ Catfishing is when someone sets up a fake online identity and uses it to trick and control others. Often they do it to scam people out of money, blackmail them or harm them in some other way – eSafety Commissioner, 2025.

Gender-Based Abuse

Gender-based abuse has become a pervasive reality in online spaces, with misogyny shifting from niche forums into the mainstream. Influencers such as Andrew Tate, Sneako, and the hosts of the Fresh and Fit podcast (Myron Gaines and Walter Weekes) attract millions with content that openly devalues women. Tate, a self-proclaimed misogynist, has described women as 'empty vessels', while Myron Gaines has promoted similar views in his book 'Why Women Deserve Less'.

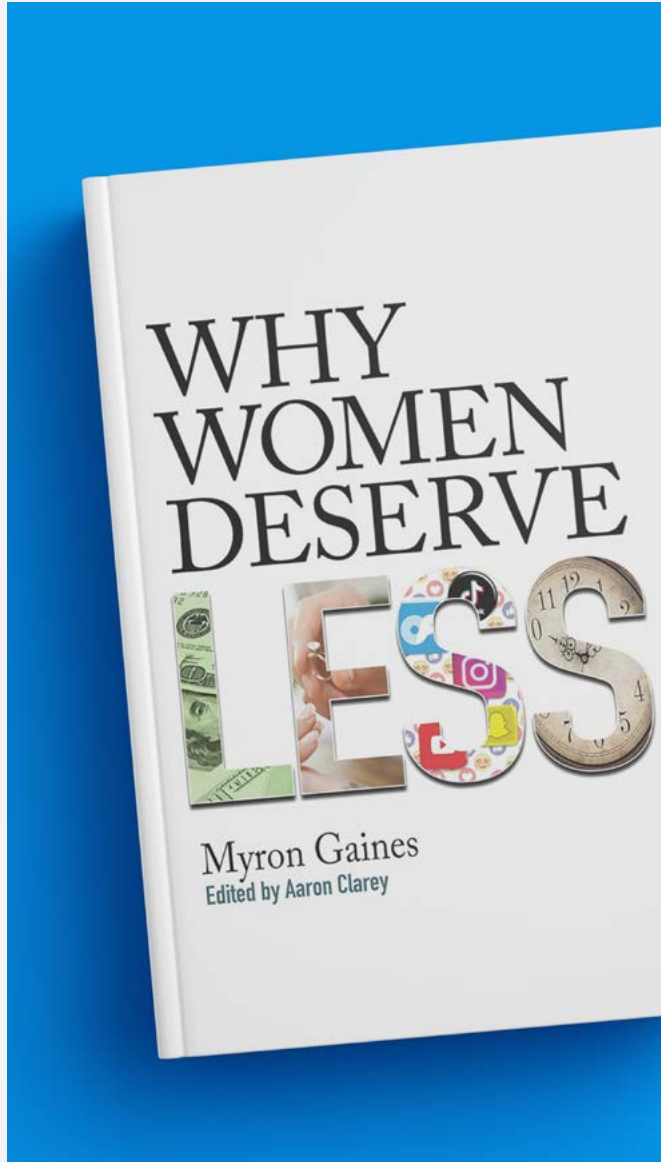
These messages are consumed as entertainment and advice by largely young, male audiences.

Research from the University of Kent and University College London found that social media platforms can quadruple the visibility of misogynistic material within five days, particularly on TikTok (UCL, 2024). Further research by Women's Aid (2023) found that this content influences attitudes - **teenagers exposed to Tate's material were five times more likely to believe that hurting others was acceptable.**

This mirrors findings by the University of Glasgow who surveyed over 13,000 pupils and found that 26% of boys said sexual harassment does not count if it is a joke - compared with only 7% of girls (Mitchell et al., 2025). For girls, the impact of constant exposure to misogyny is often felt as pressure to self-censor, withdraw from platforms, or conform to harmful norms. This undermines confidence and self-worth and contributes to a culture where harassment and inequality are normalised.

“teenagers exposed to Tate's material were five times more likely to believe that hurting others was acceptable.”

Women's Aid (2023)



Pornography

By the age of 11, more than a quarter of children have already been exposed to pornography ([Children's Commissioner, 2025](#)). Research by the [Sexual Exploitation Research & Policy \(SERP\) Institute \(2024\)](#) found that boys most often turned to pornography to learn 'what to do', while girls described seeking it out to understand 'what was expected of them'. This is a concern given that the content they encounter is overwhelmingly aggressive.

SERP reported that 94.4% of scenes in popular pornographic videos depict aggression towards women, and in over 95% of those cases women are shown responding neutrally or with pleasure. This creates a powerful message for young viewers that aggression and degradation are not only normal but something women should accept and even enjoy. The impact is particularly harmful for girls, with many describing pressure to replicate what they see, reporting distorted body image, anxiety about sexual expectations, and harmful ideas about consent and intimacy ([Children's Commissioner, 2023](#)).

The accessibility and extreme nature of pornography today is shaping the sexual development of young people in ways that normalise violence and undermine healthy relationships.

Body Image

Children and young people can encounter harmful material on eating disorders, self-harm, and extreme body ideals simply because it exists in abundance online. [The Centre for Countering Digital Hate's 'Deadly by Design' study \(2022\)](#) showed that TikTok accounts created at age 13 were recommended suicide content within 2.6 minutes, eating disorder content within 8 minutes, and further videos relating to body image every 39 seconds.

The tragic case of 14-year-old Molly Russell illustrates how the risk of viewing this kind of content can escalate. In the months before her death, Pinterest's algorithm generated emails recommending self-harm content directly to her ([Pinterest, 2022](#)). The coroner concluded that the online material she viewed contributed to her death and described it as '*not safe*' ([BBC, 2022](#)).

The impact of this type of exposure is particularly acute for girls. NHS data shows that they are four times more likely than boys to be affected by eating disorder and self-harm content ([NHS England, 2023](#)).

Young people report worsening symptoms after viewing this material, as well as desensitisation that normalises harmful behaviours. For many girls, it drives dissatisfaction with their bodies, and reinforces cultural pressures that links self-worth to their physical appearance.



Comparative Learning

This section draws on practice examples from comparative organisations. These case studies do not serve as audits of the organisations themselves but as learning opportunities, highlighting approaches, challenges, and solutions that can inform The Girls' Brigade's digital journey. The insights have been carefully reviewed, and any relevant learning has been translated into actionable recommendations within this report.

This ensures that the lessons shared here are not adopted at face value but are considered within the specific context of The Girls' Brigade's ethos, safeguarding framework, and the needs of girls and young women in the UK.

Case Study: SPACE Online Youth Group

Context and Evolution

SPACE, a youth service based in Devon, moved its work online during the pandemic. Rather than building a bespoke app, the team adopted 'Discord' because young people already knew and used the platform. After initial challenges with staff confidence and multiple fragmented servers, SPACE consolidated into a single county-wide server. The service now runs three sessions a week for 13-19 year-olds, supported by a Minecraft server and additional YouTube content to help young people familiarise themselves with the platform.

This model has proven particularly attractive to neurodivergent and LGBTQ+ young people, who now make up the majority of participants (**around 75% and 60% respectively**). Many attend because online environments feel safer or more manageable than physical clubs, and offer them a vital bridge to social connection.

Safeguarding Challenges

Running a youth service on a platform like Discord brought unique safeguarding issues. SPACE encountered incidents such as grooming attempts between older and younger teens, peers posting pornography after accounts were hacked, and young people impersonating staff by changing their usernames. Typed disclosures in group chats also presented difficulties, as sensitive information could instantly be seen by all members. Leaders had to adapt quickly, implementing clear procedures **such as**:

- Giving all participants anonymised usernames.
- Collecting minimal personal data.
- Using platform security tools (e.g. locked rooms, moderator powers).
- Training staff to respond swiftly to disruptive or harmful behaviour.

They also addressed risks in participants' physical environments, for example, reminding families about appropriate backgrounds to avoid incidents such as younger siblings inadvertently appearing nude on camera.

Inclusion and Accessibility

SPACE's digital model broke down barriers to access for young people who struggled to attend physical sessions. Options to engage by voice or text allowed young people with social anxiety, Special Educational Needs and/or Disabilities (SEND), or communication differences to take part comfortably. Online spaces also created opportunities for youth-led design, with young people influencing how sessions were run and what platforms or features were used.



Learning for The Girls' Brigade

The SPACE experience highlights that online youth work requires the same safeguarding provision as face-to-face sessions, but with adapted tools. **Key lessons include:**

- **Platform choice matters** - selecting spaces young people already use increases accessibility, but staff training and confidence are essential.
- **Procedures must be clear** - from security settings to handling disclosures, leaders need agreed steps to reduce harm.
- **Inclusion is a strength** - online youth work particularly engages neurodivergent, LGBTQ+ young people, and others who may struggle to engage in a face-to-face setting.
- **Boundaries extend offline** - young people's home environments can inadvertently create risks and leaders must be both proactive and reactive to this.
- **Youth voice is central** - co-designing digital offers with participants ensures it remains relevant and encourages sustained engagement - both of which are particularly important in an ever-changing digital world.

Case Study: GB Connect

Context

Girls' Brigade Australia has been running GB Connect, a weekly online programme, for several years. Sessions last around an hour and are hosted on Zoom, with groups ranging from two to fifteen participants. This provision particularly benefits girls who live in remote areas, including those educated through the School of the Air, who might otherwise miss out on the social interaction youth groups provide.

Integration with face-to-face delivery is limited, though girls can still achieve badges through online participation. Occasionally, those who join GB Connect also attend in-person camps, but for many, the digital offer is their primary form of engagement.

Safeguarding protocols include always having two leaders present, requiring a Working with Children Check⁶, safeguarding training, a signed code of conduct, and two referees for staff. Leaders encourage cameras to be switched on but do not record sessions.

⁶The Working with Children Check is the Australian equivalent of the UK's Disclosure and Barring Service (DBS) check.

Unlike The Girls' Brigade England and Wales, there is no requirement for written parental consent.

Keeping girls engaged requires adapting traditional activities like arts and crafts. Cameras are set up to show demonstrations, and resource packs (including basic art materials) are posted to participants. This has proved effective but also costly and time-consuming, and has required fundraising to cover postage. Over time, GB Connect has developed systems such as beginner packs for new joiners, with refills sent if materials run out. This approach has allowed the programme to grow steadily.

GB Connect has successfully adapted activities for online delivery, but The Girls' Brigade England and Wales could make further specific adjustments for hearing-impaired, visually impaired, or neurodiverse young people, or strategies to reach those with limited digital access. This highlights an opportunity to draw and develop on their existing strengths in equality, diversity and inclusion to ensure accessibility is embedded from the outset in their digital offer.

Learning for The Girls' Brigade England & Wales

- **Practical resources (such as craft packs) can enhance engagement** but must be costed and scalable if online participation grows.
- **Digital safeguarding needs to be robust** - dual consent, consideration of recording protocols, and a stronger approach to recognising risks via screens would strengthen practice. Accessibility should be embedded from the start to ensure digital sessions reflect The Girls' Brigade's ethos of inclusion.
- **Differentiated sessions, for example through breakout rooms for older girls, are necessary to maintain engagement across age ranges.**
- **A pre-set curriculum, rather than weekly adaptation of in-person materials,** ensures age-appropriate, consistent and engaging delivery.



Support Worker Removed Over Abusive Snapchat Messages to 11 Year Olds

Context

In 2023, Gillian Sorbie, a pupil support worker in Fife was permanently disqualified from working in any social care or social work roles after sending abusive and inappropriate messages to two 12-year-old girls via Snapchat.

The messages included highly offensive language such as 'love you too, s**g bag', 'just you wait till tomorrow, stupid fat wh**e', and 'try not to kill yourself while I'm gone'. Alongside this, she admitted to purchasing vapes for the pupils and their friends. The General Teaching Council for Scotland found her conduct to be fundamentally incompatible with working with children and eroded trust between children and adults in positions of responsibility.

Learning for The Girls' Brigade

Maintaining appropriate online behaviour is crucial for all staff and volunteers who work with children. Instances of misconduct have demonstrated the significant risks involved, including putting children in danger and damaging the reputation of an organisation.

- **An 'Acceptable Use of Social Media' agreement** must be established and enforced for all staff and volunteers.
- **Contact with young people** should only take place in controlled, transparent spaces - never through informal or private platforms like Snapchat.
- **Boundaries in digital contact** must be absolute to protect both young people and adults in positions of trust.
- **Trust is fragile** - one safeguarding breach by a volunteer, staff member or other associated person can undermine community confidence. Strong policies, training, and oversight are essential to maintain credibility.





Zoom Meeting Security and Safeguarding

Context and Incidents

When schools, charities, and faith groups moved online during the pandemic, many turned to Zoom as a quick solution. What few anticipated was how easily outsiders could hijack sessions.

In **2020**, a legal education seminar with around 40 attendees became the target of a serious attack. About 20 minutes into the meeting, the host lost control of their screen, and explicit child sexual abuse material was broadcast to everyone present. Each time the host tried to shut it down, the footage reappeared, leaving participants trapped in a cycle of distressing content.

The **same year**, a synagogue hosting a virtual service faced a different but equally harmful attack. The session began with around 205 participants, including children, but numbers suddenly rose as uninvited users flooded in. Once inside, they unleashed a barrage of racist and antisemitic abuse in the chat. Families attending a service intended as a safe and sacred space instead, witnessed a coordinated campaign of hate.

Learning for The Girls' Brigade

- **Session links must never be shared publicly.** Access should always be controlled through passwords and direct invitations.
- **Waiting rooms** allow leaders to admit participants one by one, keeping unwanted users out.
- **Screen sharing, private chat, and unmuting should be switched off by default** and only enabled when necessary.
- **Leaders need a clear plan of action** if a session is disrupted, including how to remove offenders and reassure participants.
- **Above all, technical security is safeguarding.** Locking down settings is about ensuring girls are never exposed to abuse or harmful content in what should be a safe space.

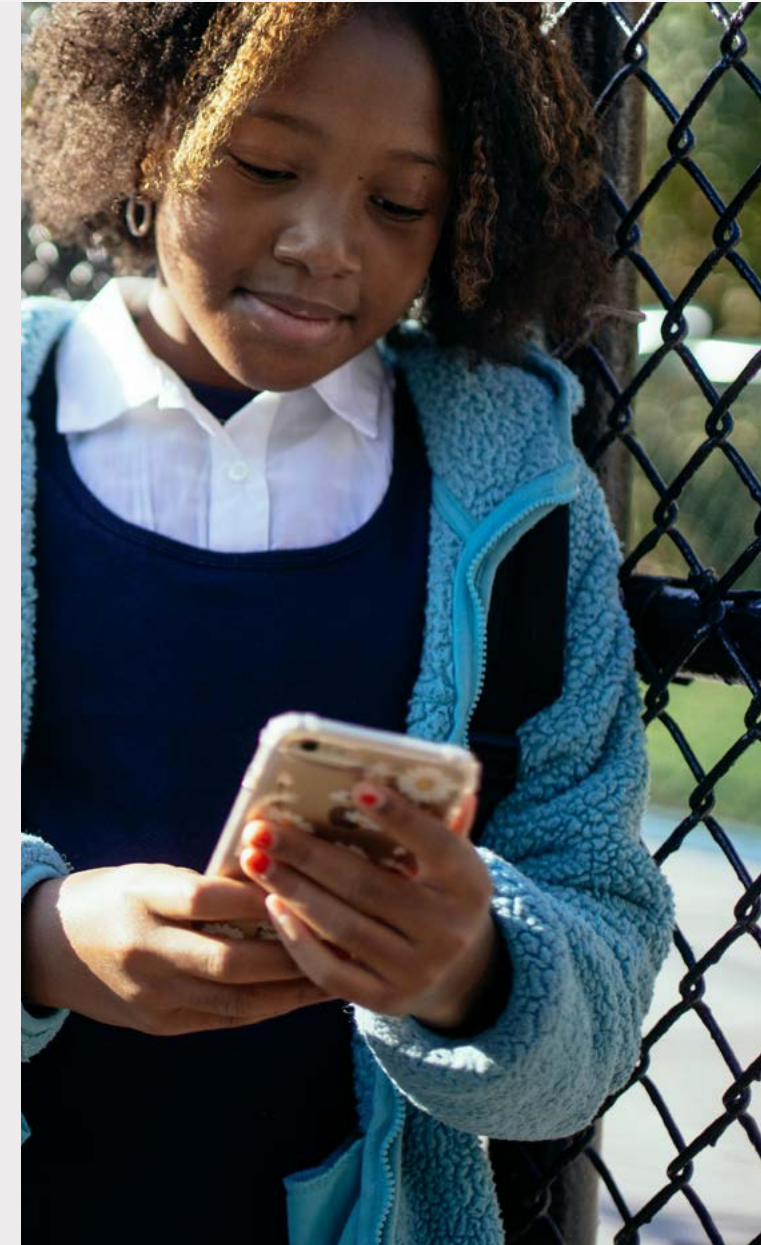
Girlguiding's Social Media Collective

Girlguiding have established a Social Media Collective - a group of young members who are specifically trained and supported to create authentic, engaging content for the organisation's social media channels, particularly TikTok. The group is managed by designated staff who provide ongoing oversight, editorial guidance, and safeguarding support. Participants receive clear instruction on online safety and responsible content creation.

This initiative strikes a good balance between empowerment and protection. It enables young people to develop valuable digital communication skills while contributing directly to how the organisation represents itself online. Crucially, it gives them a genuine voice in shaping messages that reflect the realities, humour, and creativity of their generation.

Learning for The Girls' Brigade

- **Empowering young people to take part builds confidence** and develops skills that are relevant to today's digital world.
- **Adult oversight, clear guidelines, and safeguarding support** allow creativity and safety to go hand in hand.
- **The Girls' Brigade could explore a similar Digital Ambassadors initiative** that invites a small group of older members to co-produce safe, values-led content that represents their voice and experience, overseen by the Digital Safeguarding Lead.



Recommendations for Safe and Effective Digital Youth Work

Recommendation 1: The Girls' Brigade should publish a single digital safeguarding statement of intent which has a dual purpose:

1. **Internally**, reassuring members, parents and volunteers that safeguarding remains the foundation and online work is an extension of The Girls' Brigade's ethos.
2. **Externally**, serving as a transparent, public commitment that demonstrates alignment with sector standards (NYA, OOSS expectations) and positions The Girls' Brigade ahead of the curve.

Strategy and Governance

The Girls' Brigade's position is that online work with young people will supplement existing face-to-face work. That said, introducing online youth work will inevitably raise questions and, for some, concerns that The Girls' Brigade is moving away from the traditional model they have known and valued.

Internally, publishing a statement would reassure parents, members and volunteers that safeguarding remains central to everything The Girls' Brigade does, and that digital work is not a replacement for face-to-face activities but an extension of them. This will help address fears of losing tradition, while showing that online delivery makes The Girls' Brigade more inclusive for young people who may struggle to attend in person, such as young carers, those with disabilities or those managing mental health challenges. Externally, the statement would serve as a public commitment to high standards.

Recommendation 2: In addition to the existing Designated Safeguarding Lead (DSL), The Girl's Brigade should appoint a suitably qualified and experienced Digital Safeguarding Lead with dedicated responsibility for online provision. This role should act as the focal point for advice, escalation and training, ensuring safeguarding expertise keeps pace with digital risks.

It would set out The Girls' Brigade's vision, core expectations and non-negotiables for digital youth work, signalling alignment with sector frameworks such as the NYA standards and anticipated requirements from the OOSS consultation.

This dual purpose would position The Girls' Brigade as ahead of the curve, demonstrating leadership in online safeguarding while preparing for whichever OOSS option is adopted (more information in Preparing for OOSS Requirements section).

The digital environment is complex, fast-moving and full of nuances that many well-intentioned staff and volunteers may struggle to keep pace with. Without expertise in the unique challenges posed by social media, gaming platforms, and messaging apps, there is a risk that young people may not be sufficiently protected.

Recommendation 3: The Girls' Brigade should adopt a phased approach to the expansion of its online youth work provision, ensuring safety and quality are embedded before scale. Both phases should build on the insights from the pilot discussion groups with 14-18 year olds and the recommendations in this report.

A Digital Safeguarding Lead would provide that expertise, ensuring The Girls' Brigade always has someone who understands both the technology and its safeguarding implications. For example, if a girl reported peers sharing nude images in a group chat, but parental searches of devices showed no trace, a Digital Safeguarding Lead would recognise that the group may have been deleted, or that the images could have been converted into Snapchat 'stickers' or migrated to another platform. Insights such as this one are essential to interpreting disclosures correctly and acting in a way that prevents harm being minimised or overlooked.

Rolling out online delivery across a volunteer-led organisation requires sensitivity. Not all leaders will feel equally confident in digital environments and mandating immediate participation risks creating resistance or disengagement. A phased approach reduces this risk, mirroring lessons from SPACE Online Youth Work and the NYA's Digital Youth Work Standards (2025), which emphasise piloting, reflection, and gradual capacity-building.

This phased approach will help give volunteers time to understand the functions available on the platform to conduct safe online engagement.

Phase 1 – Foundation and Design

Phase 1 should focus on creating a safe, workable model with a small group of willing and digitally confident volunteers. These volunteers should receive mandatory digital safeguarding training and ongoing support from the Digital Safeguarding Lead. Young people should be directly involved in co-designing the structure of sessions, helping shape curriculum content.

During this stage, The Girl's Brigade should also draft and test all policies and procedures, including consent protocols, safeguarding escalation routes, session security, and accessibility measures. A register of risks, trends and themes should be maintained throughout to capture issues and adjustments in real time.

Phase 2 – Expansion and Enhancement

Phase 2 should begin only after a formal evaluation of Phase 1, drawing on structured feedback from young people, parents/carers, and volunteers. Building on proven safeguarding and engagement protocols, The Girls' Brigade can widen access to a broader age range and more groups nationally. At this stage, The Girls' Brigade should consider how they develop their 'Safeguarding for Online Work in The Girls' Brigade' to include lessons from phase 1, translating these into processes. The Girls' Brigade could also expand their digital interactivity (for example, by piloting new platforms or introducing breakout groups). Phase 2 could additionally embed features of their online provision into The Girls' Brigade's core framework, for example through the creation of an 'Online Safety and Digital Resilience Badge'. Trustee oversight and governance reporting should continue, ensuring that growth does not dilute safeguarding standards.

Recommendation 4: Strengthen governance oversight by ensuring trustees receive regular reports on digital youth work and associated safeguarding, with responsibilities clearly allocated at Board level. Safeguarding roles should be visible on The Girls' Brigade's website and in all safeguarding materials.

Making governance robust and visible is about demonstrating to girls, parents and volunteers that digital youth work is being overseen with the same rigour as face-to-face activities. Trustees must be equipped with regular, clear reporting so they can ask the right questions and ensure standards are upheld.



This matters in a context where girls are disproportionately targeted online, and where parents are acutely aware of risks such as image-based abuse or grooming. Visible safeguarding roles on The Girls' Brigade's website and materials will provide assurance to families that there are people to turn to if concerns arise, and give volunteers confidence that issues raised in online sessions will be backed by a credible and accountable structure at a national level.

Recommendation 5: The Girls' Brigade should develop and maintain a risks, trends and themes dataset for digital delivery that captures real-world learning from pilots and ongoing practice. This should be updated regularly so that risks are actively monitored and mitigated.

As The Girls' Brigade adapts to online delivery, challenges will emerge. The risks, trends and themes dataset should capture those lessons and create a shared memory that prevents important information being lost when staff or leaders change. It also means trustees and senior leaders can see where risks are recurring and where additional support or training is needed.

In the online world, where harms such as sextortion, misogynistic abuse or image-sharing can appear suddenly and escalate quickly, a live risks, trends and themes dataset ensures The Girls' Brigade can act before isolated incidents become patterns. Regular updates will keep volunteers confident that their concerns are taken seriously and will help the organisation to refine practice as online delivery expands.

Recommendation 6: Ensure that safeguarding incidents occurring during digital sessions are reported to the Charity Commission as Serious Incident Reports where they meet the relevant threshold.

Any incident that results in, or poses a significant risk of, harm to a child or adult at risk (whether through online interaction, content sharing, or digital misconduct) should be assessed against the Charity Commission's Serious Incident Reporting criteria. Reporting such incidents ensures that emerging risks are captured and addressed within the the organisation's risks, trends and themes dataset (**see recommendation 5**).

Volunteer and Staff Capacity

Recommendation 7: As part of its roll out of online delivery, The Girls' Brigade should introduce mandatory digital safeguarding training for staff and volunteers on online harms (e.g. AI-generated imagery, sextortion, grooming, harmful content). Training should be scenario-based and use case studies to build confidence, and in line with The Girls' Brigade's phased roll out of online youth work.

Training is one mechanism through which safeguarding culture becomes safeguarding practice. The Girls' Brigade's *'Life to the Full'* framework already sets a strong foundation, but it does not yet address the specific and fast-moving risks of online harms (see Women and Girls in the Digital World section of this report). Without targeted training, volunteers may lack the confidence to recognise and respond to issues such as AI-generated imagery, sextortion, or misogynistic abuse.

The NYA's Digital Youth Work Standards (2025) emphasise digital safeguarding competence as central to safe online delivery, while Working Together to Safeguard Children (2023) requires training to be tailored to the risks children face. Mandatory digital safeguarding training would bridge this gap.

This training should be scenario-based, drawing on real-world case studies, and delivered in step with The Girls' Brigade's phased roll-out of online youth work (see recommendation 3). The new Digital Safeguarding Lead should oversee its design and ensure it stays responsive to emerging trends.

Recommendation 8: The Girls' Brigade should introduce an 'acceptable use' agreement for all staff and volunteers, including explicit boundaries on social media use and digital contact with young people.

The Child Protection in Sport Unit (CPSU) advises that *"any online engagement with children and young people should be carried out on public pages/groups or via their parents and carers"*, and warns against using private, encrypted channels for one-to-one contact (CPSU, 2025). The NSPCC (2022) emphasise the importance of having a code of conduct that defines acceptable behaviour for those working with young people and protecting volunteers from potentially compromising interactions.

The current *'Safeguarding for Online Youth Work in The Girls' Brigade'* document serves as a strong reference point for staff and volunteer understanding of their own online interactions. However, as The Girls' Brigade expands into digital youth work, maintaining clear boundaries between personal and professional contact is essential. Introducing an 'acceptable use' agreement ensures that all staff and volunteers not only understand these expectations, but that they are reminded of them, and pledge to adhere to them. It not only safeguards young people by setting clear digital boundaries but also protects volunteers by providing a framework that avoids misunderstandings.

Recommendation 9: The Girls' Brigade should prohibit unmoderated digital contact between staff/volunteers and young people through personal devices, email, or social media. All communication should take place through platforms which The Girls' Brigade approve, with safeguarding oversight in place.

Unmonitored contact between staff or volunteers and young people on personal channels (e.g. private messaging on social media, personal mobiles, or emails) creates significant safeguarding risks. Case studies of misconduct (e.g. inappropriate Snapchat contact by youth workers) highlight how blurred boundaries can undermine trust and expose children to harm. For The Girls' Brigade, the safest approach is to require that all online communication happens only through approved, monitored platforms (e.g. Teams, Zoom, or email accounts managed by The Girls' Brigade) where policies and safeguarding oversight apply. Staff and volunteers should receive clear guidance on what is and is not acceptable, reinforced through an Acceptable Use Agreement (**see recommendation 8**).

As The Girls' Brigade's digital offer grows, the organisation may also consider providing specific communication accounts or devices for leaders, though clear communication of expectations will often be sufficient. This would not exempt leaders from the existing rules around appropriate communication and ensuring visibility of all online interactions with young people.

Operational Safeguarding Measures

Recommendation 10: The Girls' Brigade should adopt a three-tier consent process for online sessions that reflects UK legislation and ensures safeguarding compliance without creating unnecessary barriers to participation. **This could take the following structure:**

- **Under 13s:** written parental/carer consent must be obtained (via a simple digital or paper form). At the start of the session, leaders should also check the child's verbal agreement to take part, phrased in age-appropriate language.
- **Ages 13–15:** written parental/carer consent must be secured, and the young person must also provide their own written/digital consent (e.g. ticking a box). Leaders should then carry out a short verbal consent check in the first session to confirm understanding of expectations.
- **Ages 16–17:** the young person's written/digital consent should be the primary requirement. Parents/carers should normally be informed unless doing so would put the young person at risk, consistent with Gillick competence.⁷

⁷Gillick competence refers to a legal principle from Gillick v West Norfolk and Wisbech Area Health Authority [1986] AC 112 (HL), which confirmed that children under 16 can make their own informed decisions if they have enough understanding and intelligence to fully grasp what is involved.



The proposed model will give The Girls' Brigade a framework that is both legally compliant and practical for engaging young people online. It balances three priorities - safeguarding legislation and guidance, young people's autonomy, and the reality that the opportunity for engaging a young person online can be fleeting.

Under the **Data Protection Act 2018**, the 'digital age of consent' is set at 13 for data processing under **UK GDPR**. This allows children aged 13 and above to consent to their data being used by online services. However, this does not override the **Children Act 1989**, which recognises all under-18s as children and places responsibility for their wellbeing with parents and carers. In safeguarding terms, parental consent remains the standard up to 16.

For 13-15s, dual consent reflects this balance. Parents provide formal consent in line with safeguarding law, while young people give their own explicit agreement - modelling respect for their autonomy at the very age when online risk can increase (due to their eligibility to access many social media platforms from age 13).

For 16-17s, the principle of Gillick competence applies. At this age, young people are generally presumed able to make informed decisions about their participation. Their consent should therefore be the primary requirement, with parents normally informed unless doing so would put the young person at risk.

Digital forms should be short and mobile-friendly, and leaders should reinforce them with a brief verbal consent check at the start of sessions. By keeping the process streamlined, The Girls' Brigade avoids creating barriers that could deter a girl from joining at the moment she discovers the organisation online. At the same time, it embeds a culture where young people learn that consent is active, ongoing, and central to their safety - modelling exactly the behaviour that helps protect them in wider digital life.



Recommendation 11: The Girls' Brigade should provide accessible onboarding resources, such as short videos or interactive guides, that explain how to use chosen platforms safely and effectively. These should cover how sessions work, what behaviour is expected, and where to go for support, including how to contact the Digital Safeguarding Lead. To ensure all young people can engage, materials should be designed with accessibility in mind, for example by including subtitles, Makaton, clear visuals and audio descriptions.

Providing clear onboarding resources is a practical way of reducing barriers to participation while maintaining safeguarding standards. Just as the consent process must be clear enough not to deter a girl who discovers The Girls' Brigade online, onboarding materials should make it easy to understand both the opportunities and responsibilities of joining.

Short videos or interactive guides can form part of an introductory package that explains the platform being used (for example Teams or Zoom), sets out expectations for safe participation, and directs users to the appropriate point of contact such as the Digital Safeguarding Lead if they need help. The use of Makaton, subtitles, voiceovers and accessible formats will allow all young people to engage confidently, including those with SEND or additional needs.

Recommendation 12: The Girls' Brigade should adopt a clear policy on recording online sessions, with the default position being that sessions are not recorded. Where exceptional circumstances make recording necessary, this must be justified through a Data Protection Impact Assessment, approved in advance, and fully compliant with UK GDPR and safeguarding law. Any recording should be strictly time-limited, securely stored, and accessed only by authorised personnel, with clear retention and deletion protocols in place.

Whilst recording sessions may appear as an additional layer of safeguarding for staff and young people, there is no legal requirement to record youth sessions. Staff must utilise appropriate ratios and always have a minimum of two staff within any online engagement with young people. If The Girls' Brigade choose to record, they will be processing children's personal data, so it must be necessary and proportionate (UK GDPR / Data Protection Act 2018), with a clear lawful basis and Article 5 safeguards, for example, purpose limitation, minimisation, storage limitation or security.

The Girls' Brigade should not rely on consent as its default lawful basis. If special category data are likely to be captured (e.g. religious belief inferred from participation or health information revealed), you will also need an Article 9 condition, commonly '*safeguarding of children and individuals at risk*' under the Data Protection Act 2018 Sch.1 para 18, with an appropriate policy document.

A Data Protection Impact Assessment (DPIA) is strongly advised before undertaking any activity online with new technology or systems that may include the recording of children online, to evidence necessity, proportionality, risks and mitigations.

Recording Guidance

- 1. Default processes:** avoid recording online youth sessions. Use a minimum of two adults to facilitate sessions, have clear ground rules and keep detailed notes as your primary safeguarding controls.
- 2. Exceptional recording:** only where a specific, documented reason exists (e.g. safeguarding review, serious incident capture, essential accessibility need). Complete a DPIA before introducing technology that may include recording children, and name the lawful basis and Article 9 condition. Provide short, child-friendly privacy information at sign-up and on-screen notification at the start of any recorded session.
- 3. Minimise imagery of U18s:** use blurred backgrounds or record the facilitator view and shared materials rather than gallery view. Do not capture private chat unless needed for safeguarding evidence.
- 4. Security and retention:** store recordings on approved, encrypted systems, restrict access to those with a defined role, time-limit retention (set and publish a short retention period), and never allow staff to record on personal devices.
- 5. Alternatives:** if the aim is training, supervision or quality assurance, consider live drop-ins by supervisors, post-session debriefs, and redacted notes rather than recording children.

Recommendation 13: All online sessions should have a minimum of two appropriately vetted and trained adult leaders present. Ratios should be age-appropriate, with smaller groups or breakouts for older teenagers where conversations may be more sensitive.



Requiring at least two adult leaders in every online session protects both young people and staff. Lone working in digital spaces carries significant risks. If a session is not recorded, a leader can be left without accountability, leaving them exposed to allegations. The presence of a second adult also provides support if a disclosure is made, ensuring that one leader can respond directly to the child while the other manages the group. Additionally, a young person may suddenly drop offline, show signs of distress, or reveal something concerning in the background of their video. Having two leaders ensures that one adult can engage sensitively with the individual while the other maintains oversight of the wider session.

This approach reflects expectations set out in Working Together to Safeguard Children (2023), which emphasises the importance of organisational arrangements that prevent unsupervised contact between adults and children. It also aligns directly with the NYA's Digital Youth Work Standards (2025), which emphasise that digital youth work must be underpinned by the same safeguarding principles as face-to-face provision, including safe ratios, transparency, and accountability.

For older teenagers, smaller group ratios or breakout rooms may be appropriate to create safe spaces for more sensitive conversations. However, the principle of dual leadership remains essential in all contexts.



Recommendation 14: The Girls' Brigade should require all leaders to have their cameras on during online sessions and encourage young people to do the same. However, participation must not be conditional on camera use. Where a young person chooses to keep their camera off, leaders should use alternative methods (such as verbal check-ins, chat participation, or follow-up contact) to confirm their presence and wellbeing.

Camera use in online sessions is both a safeguarding and an engagement issue. When young people have cameras on, leaders can verify attendance, read body language, and spot early signs of distress, much as they would in face-to-face youth work. It also helps to develop trust and a sense of community.

The NYA's Digital Youth Work Standards (2025) highlight that online youth work must combine safety with accessibility, recognising that not all young people can or will participate in the same way. Some may lack a private space at home, feel unsafe revealing their surroundings, or experience digital exclusion. For these reasons, while The Girls' Brigade should encourage cameras to be switched on, no girl should be excluded if she chooses otherwise.

Instead, leaders should explain why camera use is encouraged and provide alternative ways to engage if a participant keeps theirs off - for example, regular verbal check-ins, use of the chat function, or direct follow-up if a young person becomes unresponsive. Leaders themselves should model good 'offline' practice by keeping cameras on at all times - just as leaders would always be visible to children in person.

Curriculum and Resources

Recommendation 15: The Girls' Brigade should develop a structured digital curriculum for online delivery that embeds safeguarding by design. **This curriculum should:**

- **Reflect** on lessons from piloted sessions.
- **Provide** consistent, age-appropriate content across all groups.
- **Address** key risks facing girls online, including intimate image abuse, sextortion, pornography, misogyny, and harmful content.
- **Be evidence-informed** and developed in consultation with safeguarding experts.
- **Be co-designed** and co-produced with the young people that The Girls' Brigade serves.

A structured digital curriculum will ensure that all members of The Girls' Brigade receive a consistent and safe programme of work. The NYA's Digital Youth Work Standards (2025) highlight the need for planned, evidence-informed content in digital settings. For The Girls' Brigade, that means explicitly addressing harms disproportionately affecting girls, such as the ones outlined in this report. In addition, the curriculum should directly address online safety 'basics', such as understanding privacy settings, what information should be private and what is safe to share online or how to reset algorithms that are showing upsetting or inappropriate content.

Consulting safeguarding experts provides a level of reassurance of accuracy and credibility, while co-design with girls themselves will make sure the content resonates with lived experience.

Recommendation 16: The Girls' Brigade should review how physical resources are integrated into online delivery, ensuring any packs or materials are costed and scalable.

Experience from The Girls' Brigade Australia shows that providing physical resource packs alongside online sessions can support engagement but is often expensive and time-intensive. As The Girls' Brigade develops its digital offer, it will need to decide which activities require physical resources, how these are distributed, and how costs will be managed if participation grows. Factoring this into budget and planning early will prevent resource provision becoming a barrier to sustainability.

Recommendation 17: The Girls' Brigade Support Centre should maintain oversight of the standardised introductions used in all online sessions, ensuring they consistently cover safeguarding essentials. These should include reminders about what is appropriate to share in the group, where and when sensitive issues can be raised safely, who to contact if something is bothering them, and that screenshots and recordings are not permitted.

Setting clear expectations at the start of each session is a simple but powerful safeguarding measure. Typed disclosures in group chats can expose all participants to sensitive or distressing information. Leaders must be prepared to respond appropriately, but children and young people also need to know there are safer routes for sharing concerns. Screenshots and recordings create risks if inappropriate or private content is captured (such as siblings appearing in the background).

Whilst maintaining oversight of these introductory messages at the Support Centre level is important for consistency, it will also be important to remain responsive to the experiences of local volunteers who may help to identify if additional points are needed in certain contexts, allowing the national script to be refined and kept relevant across all groups.



Recommendation 18: The Girls' Brigade should create a safeguarding signposting guide for leaders. The guide should be concise, easy to access during sessions, and designed as a quick-reference tool that complements The Girls' Brigade's internal escalation process.

The purpose of the signposting guide is to support leaders, not to replace statutory reporting. **Its function is twofold:**

1. **To remind** leaders of The Girls' Brigade's internal escalation routes when a safeguarding concern arises.
2. **To equip** leaders with accurate information about trusted UK helplines and specialist services they can signpost young people to, either during or after a disclosure.

The guide should cover organisations such as (but not limited to):

- **Childline** – 24/7 confidential support for children and young people.
- **Report Remove (IWF/Childline)** – a service for children to request removal of intimate images.
- **NSPCC Helpline** – advice for adults who are concerned about a child's welfare.
- **The Mix** – support for under-25s on issues including relationships, mental health, and online safety.
- **Samaritans** – crisis support for anyone experiencing suicidal thoughts or distress.

Access, Security and Inclusion

Recommendation 19: The Girls' Brigade should continue to secure online sessions by configuring platforms safely and ensuring leaders are trained to respond to disruptive incidents. This should include:

- Maintaining the existing practice of not sharing links publicly to online sessions and ensuring they operate on an invite-only basis.
- Manually verifying all usernames.
- Using passwords, waiting rooms, co-hosting, and locked meetings.
- Disabling screen sharing, private chat, and whiteboards for participants.
- Having a clear contingency plan for disruptive incidents (e.g. impersonation, harmful content, or hacking).

Online youth work relies on digital platforms that can be vulnerable to misuse if not carefully configured. Unsecured online sessions have repeatedly been hijacked by outsiders ('Zoom-bombing'), with incidents reported by schools and youth groups during the COVID-19 pandemic. Risks include the sharing of harmful material, targeted abuse, and young people being exposed to inappropriate content. The NYA's Digital Youth Work Standards (2025) emphasise safe digital environments as non-negotiable, requiring platforms to be configured with safeguarding in mind.

By maintaining existing measures such as keeping joining links private and other simple but consistent security measures, The Girls' Brigade can minimise risks and demonstrate to parents and partners that safeguarding is taken seriously. A clear contingency plan ensures that if disruption does occur, leaders can act quickly, for example, by removing offenders, pausing the session, and following up with safeguarding procedures.

Recommendation 20: The Girls' Brigade should continue to ensure all online delivery is accessible from the outset. This includes practical adaptations for young people with SEND, hearing/visual impairments, and neurodiverse needs. Accessibility measures should be embedded in planning, not added retrospectively, and should build on The Girls' Brigade's recognised strengths in equality, diversity and inclusion.

Accessibility is a legal and safeguarding requirement. **The Equality Act 2010** requires organisations to make reasonable adjustments and prohibits discrimination on the basis of disability. **The Children and Families Act 2014** strengthens this duty, mandating support for children with SEND and emphasising the need for inclusive provision up to age 25. Statutory guidance reinforces these obligations: Working Together to Safeguard Children (2023) highlights that children with disabilities are more vulnerable to harm, while the SEND Code of Practice requires early identification and proactive adjustments.

Accessibility by design models The Girls' Brigade's ethos of inclusion and ensures no girl is excluded from digital participation due to barriers that could be anticipated and addressed. **Examples of good practice include:**

- **Providing closed captions** and transcripts on all video-based content.
- **Ensuring platforms are compatible** with screen readers and accessible colour contrast.
- **Offering flexible participation methods** (e.g. chat functions or breakout spaces) for young people who may struggle with group video.
- **Training leaders** to understand and respond to accessibility needs sensitively.
- **Having instructions in both written and verbal formats.**

Recommendation 21: The Girls' Brigade should embed structured evaluation into online sessions. Feedback should be gathered from young people, parents/carers, and leaders through short surveys, focus groups, and debriefs. Insights should be collated centrally to refine delivery and inform wider rollout.

Evaluation is essential to ensure The Girls' Brigade's online delivery develops in a way that is safe, engaging, and responsive to the needs of girls and young women. **For The Girls' Brigade, evaluation of pilots should be structured and multi-layered:**

- **Young people:** short, accessible surveys immediately after sessions (using mobile-friendly forms) to capture impressions of safety, engagement, and relevance; followed by optional focus groups to explore issues in more depth. Where possible, anonymity should be used to increase the honesty and rate of responses (proportionate to age and sensitivity of topic).
- **Parents/carers:** brief questionnaires on their confidence in The Girls' Brigade's safeguarding approach, consent processes, and communication.
- **Leaders/volunteers:** structured debriefs capturing what worked, what was challenging, and any suggestions for improvement.

Collecting feedback from all three groups ensures that The Girls' Brigade has a rounded picture of how online delivery is experienced and prevents blind spots that could leave young people unprotected or disengaged.

This evaluation cycle should be repeated after every phase of the roll out, and at regular intervals thereafter, with findings documented in a central learning log and shared with trustees.

Recommendation 22: The Girls' Brigade should develop a clear protocol for evidence-gathering in online sessions. This must ensure that when quotes, polls, or screenshots are captured for evaluation or reporting, young people's names, faces, and identifiable details are anonymised or removed. Where this is not possible, the content should be recreated in an anonymised format before wider use.

Online platforms such as Teams or Zoom allow leaders to capture feedback through polls, Q&A functions, and chat contributions. However, screenshots can inadvertently capture names, images, or other identifiers. If shared without adaptation, this risks breaching confidentiality, eroding trust, and exposing young people's identities. To mitigate this during feedback activities, leaders can instruct young people to use neutral usernames, or alternatively, screenshots can be edited or recreated with identifying details removed. This ensures that the authenticity of girls' views is retained without risking privacy.

Recommendation 23: The Girls' Brigade's should introduce an Online Safety and Digital Resilience Badge as part of its wider structured digital curriculum. The badge should be co-designed with young people and introduced once The Girls' Brigade's approach to online delivery and curriculum has reached a mature point.

Badges are already a familiar and valued part of The Girls' Brigade's programme, giving members visible recognition for their learning and achievements. An Online Safety and Digital Resilience Badge would provide a clear, tangible way of celebrating young people's growth in navigating the digital world. **This badge should:**

- **Emerge as a next step** once The Girls' Brigade's online delivery model and digital curriculum are established and tested, ensuring the badge reflects practice that is already embedded.
- **Complement, not duplicate, drawing its learning outcomes directly from the curriculum** but translate them into accessible, activity-based challenges.
- **Normalise conversations about online harms** such as intimate image abuse, sextortion, and harmful content, making them part of everyday youth work.
- **Model safeguarding by design**, with the content co-designed by The Girls' Brigade members themselves to ensure accuracy and relevance.
- **Celebrate digital competence**, allowing girls to earn recognition for developing skills that keep them and their peers safer online.

By introducing the badge at a later stage, The Girls' Brigade ensures it builds on a foundation of established practice, turning safeguarding education into something visible and motivating for members, while reinforcing its wider commitment to preparing girls for life in the digital age.



Example of Design

Preparing for Out-of-School Settings (OOSS) Requirements

What Each Option Could Mean for The Girls' Brigade and its Digital Offer

At the time of writing, the Department for Education is consulting on three possible approaches to strengthen safeguarding in Out-of-School Settings: mandatory registration or regulation, an accreditation or 'kitemark' scheme, and an information-led model that improves guidance for providers, parents and children. For The Girls' Brigade, the existing 'Keeping children safe in out-of-school settings: code of practice' remains non-statutory and offers baseline expectations.

1. Registration and/or Regulation

If the government opts for registration or regulation, The Girls' Brigade will need to provide named safeguarding leads, safer recruitment evidence, and details of its delivery, including online activity. Regulation could extend this to inspections and formal complaints processes. For parents, this creates consistency and confidence and for The Girls' Brigade, it increases visibility on a national register. The organisation already has a safeguarding framework in *'Life to the Full'* and is undergoing external assessment with 31:8, so it can evidence compliance quickly.

The challenge is the added administration - collating risk assessments, training logs, consent processes, and incident records for every online session. These requirements are not abstract; they are already reflected in the NYA's Digital Youth Work Standards, which make clear that risk management and data protection must apply equally online. Building a single digital 'evidence pack' now will ensure The Girls' Brigade is inspection-ready if regulation comes, and even if it does not, that discipline will strengthen practice and demonstrate leadership in the sector.

2. Accreditation and Partnerships (Kitemark)

A kitemark scheme would allow providers to be voluntarily assessed against agreed safeguarding standards, earning a badge of trust parents can see. For The Girls' Brigade, this offers a real opportunity to validate its safeguarding culture publicly and showcase its online safety credentials. The benefits of this option are clear - in a crowded sector, a kitemark would help parents, funders, and partners see The Girls' Brigade as a safe choice. Additionally, it will align with the NYA Digital Youth Work Standards. The downside is cost and duplication: accreditation needs staff time, money, and renewal, and if multiple schemes appear, The Girls' Brigade could face competing demands or requirements that later clash with registration. Similar to option 1, in digital delivery, accreditation would almost certainly require evidence of practice - policies on consent, leader ratios, accessibility for SEND, and clear procedures for handling disclosures online. Assembling that evidence pack now will build credibility with parents, strengthen governance, and ensure The Girls' Brigade is ready whichever route government takes.

3. Information-Based Approach

An information-based model would rely on stronger guidance and awareness-raising for parents, providers, and children. This is the least administratively demanding option and would give The Girls' Brigade freedom to innovate without the cost or scrutiny of external inspections or accreditation. But it also carries risk. Without enforceable standards, weaker providers could cut corners, undermining trust in the sector and leaving parents with inconsistent information on quality.

For The Girls' Brigade, this model creates an opportunity. By publishing its own digital safeguarding standards (underpinned by the NYA Digital Youth Work Standards), The Girls' Brigade could show it is not waiting for regulation to dictate expectations. A clear, public statement of safeguarding commitments would reassure parents and position The Girls' Brigade as a transparent, self-regulating organisation. If the government later shifts to registration or accreditation, this groundwork would not be wasted as it would simply place The Girls' Brigade ahead of the curve, already seen as a leader in safe digital youth work.

Recommendations for Futureproofing Against OOSS Outcomes

INEQE make the following recommendations for The Girls' Brigade to place themselves ahead of the curve and are reusable under any model. They avoid unnecessary work by building one evidence base that can be lifted into registration, accreditation or information-led expectations.

Recommendation 24: The Girls' Brigade should build a digital safeguarding evidence pack by collating the key elements highlighted throughout this report, **including:**

1. Policies specific to online sessions
2. Digital risks, trends and themes dataset
3. Training records
4. Trustee reports
5. Consent processes
6. Evaluation findings
7. Accessibility measures
8. Collated list of digital-based incidents reported to the Charity Commission as a Serious Incident Report.

In addition, The Girl's Brigade should ensure they have a standardised system for recording safeguarding incidents that occur in online sessions. This includes disclosures, chat-based concerns, and sudden drop-offs.

Recommendation 25: Trustees should commission a simple mapping exercise that shows how current and planned actions align with each possible OOSS model. This ensures The Girls' Brigade can evidence compliance under registration, accreditation, or information-based approaches without unnecessary duplication of work.

Recommendation 26: Under an information-based model, the sector risks inconsistency. The Girls' Brigade should pre-empt this by publishing its digital safeguarding statement of intent (already recommended), supported by a short public-facing guide that explains standards for online youth work.

This will reassure parents, demonstrate transparency, and set The Girls' Brigade apart as an exemplar regardless of the eventual government decision.

Recommendation 27: The Girl's Brigade should map its online practice against the NYA's Digital Youth Work Standards ('who, what, where, how'), including accessibility, youth participation, and curriculum. Using the NYA checklist will help The Girls' Brigade demonstrate continuous improvement and strengthen credibility with regulators and parents.





Conclusion

Safeguarding is fundamental to the work of The Girls' Brigade, as evidenced by its ethos of care and inclusion, the solid foundations of the *Life to the Full* framework, and its proactive approach to embedding safety in every aspect of youth work - such as the commissioning of this report.

Online harm is not a future threat. It is the lived reality for many children and young people today. Parents are looking for assurance, regulators are raising expectations, and young people are asking for safe, relevant spaces. The Girls' Brigade is well placed to meet these challenges and to lead by example.

The way ahead is not about complexity but about consistency. Doing the basics well, every time, is what builds safety, and trust. That means a clear safeguarding statement of intent, a dedicated Digital Safeguarding Lead, scenario-based training, and a phased approach that starts small, learns quickly, and scales only when safe to do so.

Operational discipline is equally important. Secure platforms, clear ground rules, appropriate ratios in every session, and accessible design as standard must all become non-negotiables. A structured digital curriculum, co-designed with young people, will ensure that The Girls' Brigade's online work is engaging as well as safe. A live risks, trends and themes dataset, and a consolidated evidence pack will keep governance strong, ensuring trustees can see risks clearly and act decisively.

Safeguarding does not change, but technology does. By embedding strong, simple processes now and building on them step by step, The Girls' Brigade can create safe digital spaces where girls are included, empowered, and protected. In doing so, the organisation will not only safeguard its own members but also set a benchmark for the wider youth sector.

List of Recommendations

Recommendation 1: The Girls' Brigade should publish a single digital safeguarding statement of intent which has a dual purpose:

1. **Internally**, reassuring members, parents and volunteers that safeguarding remains the foundation and online work is an extension of The Girls' Brigade's ethos.
2. **Externally**, serving as a transparent, public commitment that demonstrates alignment with sector standards (NYA, OOSS expectations) and positions The Girls' Brigade ahead of the curve.

Recommendation 3: The Girls' Brigade should adopt a phased approach to the expansion of its online youth work provision, ensuring safety and quality are embedded before scale. Both phases should build on the insights from the pilot discussion groups with 14 -18 year olds and the recommendations in this report.

Recommendation 4: Strengthen governance oversight by ensuring trustees receive regular reports on digital youth work and associated safeguarding, with responsibilities clearly allocated at Board level. Safeguarding roles should be visible on The Girls' Brigade's website and in all safeguarding materials.

Recommendation 2: In addition to the existing Designated Safeguarding Lead (DSL), The Girl's Brigade should appoint a suitably qualified and experienced Digital Safeguarding Lead with dedicated responsibility for online provision. This role should act as the focal point for advice, escalation and training, ensuring safeguarding expertise keeps pace with digital risks.

Recommendation 5: The Girls' Brigade should develop and maintain a risks, trends and themes dataset for digital delivery that captures real-world learning from pilots and ongoing practice. This should be updated regularly so that risks are actively monitored and mitigated.

Recommendation 6: Ensure that safeguarding incidents occurring during digital sessions are reported to the Charity Commission as Serious Incident Reports where they meet the relevant threshold.

Recommendation 7: As part of its roll out of online delivery, The Girls' Brigade should introduce mandatory digital safeguarding training for staff and volunteers on online harms (e.g. AI-generated imagery, sextortion, grooming, harmful content). Training should be scenario-based and use case studies to build confidence, and in line with The Girls' Brigade's phased roll out of online youth work.

Recommendation 8: The Girls' Brigade should introduce an 'acceptable use' agreement for all staff and volunteers, including explicit boundaries on social media use and digital contact with young people.

Recommendation 9: The Girls' Brigade should prohibit unmoderated digital contact between staff/volunteers and young people through personal devices, email, or social media. All communication should take place through platforms which The Girls' Brigade approve, with safeguarding oversight in place.

Recommendation 10: The Girls' Brigade should adopt a three-tier consent process for online sessions that reflects UK legislation and ensures safeguarding compliance without creating unnecessary barriers to participation. **This could take the following structure:**

- **Under 13s:** written parental/carers consent must be obtained (via a simple digital or paper form). At the start of the session, leaders should also check the child's verbal agreement to take part, phrased in age-appropriate language.
- **Ages 13–15:** written parental/carers consent must be secured, and the young person must also provide their own written/digital consent (e.g. ticking a box). Leaders should then carry out a short verbal consent check in the first session to confirm understanding of expectations.
- **Ages 16–17:** the young person's written/digital consent should be the primary requirement. Parents/carers should normally be informed unless doing so would put the young person at risk, consistent with Gillick competence.

Recommendation 11: The Girls' Brigade should provide accessible onboarding resources, such as short videos or interactive guides, that explain how to use chosen platforms safely and effectively. These should cover how sessions work, what behaviour is expected, and where to go for support, including how to contact the Digital Safeguarding Lead. To ensure all young people can engage, materials should be designed with accessibility in mind, for example by including subtitles, Makaton, clear visuals and audio descriptions.

Recommendation 12: The Girls' Brigade should adopt a clear policy on recording online sessions, with the default position being that sessions are not recorded. Where exceptional circumstances make recording necessary, this must be justified through a Data Protection Impact Assessment, approved in advance, and fully compliant with UK GDPR and safeguarding law. Any recording should be strictly time-limited, securely stored, and accessed only by authorised personnel, with clear retention and deletion protocols in place.

Recommendation 13: All online sessions should have a minimum of two appropriately vetted and trained adult leaders present. Ratios should be age-appropriate, with smaller groups or breakouts for older teenagers where conversations may be more sensitive.

Recommendation 14: The Girls' Brigade should require all leaders to have their cameras on during online sessions and encourage young people to do the same. However, participation must not be conditional on camera use. Where a young person chooses to keep their camera off, leaders should use alternative methods (such as verbal check-ins, chat participation, or follow-up contact) to confirm their presence and wellbeing.

Recommendation 15: The Girls' Brigade should develop a structured digital curriculum for online delivery that embeds safeguarding by design. **This curriculum should:**

- **Reflect** on lessons from piloted sessions.
- **Provide** consistent, age-appropriate content across all groups.
- **Address** key risks facing girls online, including intimate image abuse, sextortion, pornography, misogyny, and harmful content.
- **Be evidence-informed** and developed in consultation with safeguarding experts.
- **Be co-designed** and co-produced with the young people that The Girls' Brigade serves.

Recommendation 16: The Girls' Brigade should review how physical resources are integrated into online delivery, ensuring any packs or materials are costed and scalable.

Recommendation 17: The Girls' Brigade Support Centre should maintain oversight of the standardised introductions used in all online sessions, ensuring they consistently cover safeguarding essentials. These should include reminders about what is appropriate to share in the group, where and when sensitive issues can be raised safely, who to contact if something is bothering them, and that screenshots and recordings are not permitted.

Recommendation 18: The Girls' Brigade should create a safeguarding signposting guide for leaders. The guide should be concise, easy to access during sessions, and designed as a quick-reference tool that complements The Girls' Brigade's internal escalation process.

Recommendation 19: The Girls' Brigade should continue to secure online sessions by configuring platforms safely and ensuring leaders are trained to respond to disruptive incidents. This should include:

- Maintaining the existing practice of not sharing links publicly to online sessions and ensuring they operate on an invite-only basis.
- Manually verifying all usernames.
- Using passwords, waiting rooms, co-hosting, and locked meetings.
- Disabling screen sharing, private chat, and whiteboards for participants.
- Having a clear contingency plan for disruptive incidents (e.g. impersonation, harmful content, or hacking).

Recommendation 20: The Girls' Brigade should continue to ensure all online delivery is accessible from the outset. This includes practical adaptations for young people with SEND, hearing/visual impairments, and neurodiverse needs. Accessibility measures should be embedded in planning, not added retrospectively, and should build on The Girls' Brigade's recognised strengths in equality, diversity and inclusion.

Recommendation 21: The Girls' Brigade should embed structured evaluation into online sessions. Feedback should be gathered from young people, parents/carers, and leaders through short surveys, focus groups, and debriefs. Insights should be collated centrally to refine delivery and inform wider rollout.

Recommendation 22: The Girls' Brigade should develop a clear protocol for evidence-gathering in online sessions. This must ensure that when quotes, polls, or screenshots are captured for evaluation or reporting, young people's names, faces, and identifiable details are anonymised or removed. Where this is not possible, the content should be recreated in an anonymised format before wider use.

Recommendation 23: The Girls' Brigade's should introduce an Online Safety and Digital Resilience Badge as part of its wider structured digital curriculum. The badge should be co-designed with young people and introduced once The Girls' Brigade's approach to online delivery and curriculum has reached a mature point.

Recommendation 24: The Girls' Brigade should build a digital safeguarding evidence pack by collating the key elements highlighted throughout this report, **including:**

1. Policies specific to online sessions
2. Digital risks, trends and themes dataset
3. Training records
4. Trustee reports
5. Consent processes
6. Evaluation findings
7. Accessibility measures
8. Collated list of digital-based incidents reported to the Charity Commission as a Serious Incident Report.

In addition, The Girl's Brigade should ensure they have a standardised system for recording safeguarding incidents that occur in online sessions. This includes disclosures, chat-based concerns, and sudden drop-offs.

Recommendation 25: Trustees should commission a simple mapping exercise that shows how current and planned actions align with each possible OOSS model. This ensures The Girls' Brigade can evidence compliance under registration, accreditation, or information-based approaches without unnecessary duplication of work.

Recommendation 26: Under an information-based model, the sector risks inconsistency. The Girls' Brigade should pre-empt this by publishing its digital safeguarding statement of intent (already recommended), supported by a short public-facing guide that explains standards for online youth work.

This will reassure parents, demonstrate transparency, and set The Girls' Brigade apart as an exemplar regardless of the eventual government decision.

Recommendation 27: The Girl's Brigade should map its online practice against the NYA's Digital Youth Work Standards ('who, what, where, how'), including accessibility, youth participation, and curriculum. Using the NYA checklist will help The Girls' Brigade demonstrate continuous improvement and strengthen credibility with regulators and parents.

References

BBC (2020), 'Coronavirus: Racist 'zoombombing' at virtual synagogue'. Available at: <https://www.bbc.co.uk/news/technology-52105209>

BBC (2020), 'Zoom meetings targeted by abuse footage sharers'. Available at: <https://www.bbc.co.uk/news/uk-52391531>

BBC (2022), 'Molly Russell inquest: Pinterest executive admits site was not safe'. Available at: <https://www.bbc.co.uk/news/uk-england-london-62991510>

Center for Countering Digital Hate (CCDH) (2022), Deadly by Design. Available at: <https://counterhate.com/research/deadly-by-design/>

Child Protection in Sport Unit (CPSU) (2025), 'Online safety and social media: Social media best practice'. Available at: <https://thecpsu.org.uk/help-advice/topics/online-safety-and-social-media/>

Children's Commissioner (2023), 'A lot of it is actually just abuse' Young people and pornography'. Available at: <https://assets.childrenscommissioner.gov.uk/wpuploads/2023/02/cc-a-lot-of-it-is-actually-just-abuse-young-people-and-pornography-updated.pdf>

Children's Commissioner (2025), '“Sex is kind of broken now”: children and pornography'. Available at: <https://assets.childrenscommissioner.gov.uk/wpuploads/2025/08/Embargoed-Sex-is-kind-of-broken-now-Children-and-Pornography.pdf>

Department for Education (DfE) (2023) Working Together to Safeguard Children: A guide to inter-agency working to improve the wellbeing of children and young people. London: HM Government. Available at: <https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>

Department for Education (DfE) (2024) Safeguarding in out-of-school settings: Call for evidence. London: HM Government. Available at: <https://consult.education.gov.uk/out-of-school-settings-safeguarding-team/out-of-school-settings-safeguarding-call-for-evidence/>

European Union (2016) Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119, pp. 1–88. Available at: <https://www.legislation.gov.uk/eur/2016/679/contents>

Girlguiding (2023), Girls' Attitudes Survey 2023. Available at: <https://girlguidingulster.org.uk/assets/uploads/girls-attitudes-summary.pdf>

Girlguiding (2024) Girls' Attitudes Survey 2024. Available at: <https://www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2024.pdf>

Girlguiding (2025) 'One in four teens have seen pornographic deepfakes online'. Available at: <https://www.girlguiding.org.uk/about-us/press-releases/one-in-four-teens-have-seen-pornographic-deepfakes-online/>

INEQE Safeguarding Group (2025) 'Safeguarding Students: A Guide for Schools on Preventing and Responding to AI-Generated Image Exploitation'. Available at: <https://ineqe.com/2025/02/18/ai-generated-image-exploitation-school-guide/>

Internet Watch Foundation (IWF) (2024) 'Exponential increase in cruelty' as sextortion scams hit younger victims'. Available at: <https://www.iwf.org.uk/news-media/news/exponential-increase-in-cruelty-as-sextortion-scams-hit-younger-victims/>

Internet Watch Foundation (IWF) (2024) 'IWF sounds alarm for young people and parents as sharing of nudes becomes 'normalised' in UK schools'. Available at: <https://www.iwf.org.uk/news-media/news/iwf-sounds-alarm-for-young-people-and-parents-as-sharing-of-nudes-becomes-normalised-in-uk-schools/>

Internet Watch Foundation (IWF) (2025), 'AI images of child sexual abuse getting 'significantly more realistic', says watchdog'. Available at: <https://www.iwf.org.uk/news-media/iwf-in-the-news/ai-images-of-child-sexual-abuse-getting-significantly-more-realistic-says-watchdog/>

Jones, S. (2024) 'Spain sentences 15 school children over AI-generated naked images'. The Guardian. Available at: <https://www.theguardian.com/world/article/2024/jul/09/spain-sentences-15-school-children-over-ai-generated-naked-images>

Jurecic et al., (2016), 'Commentary Sextortion: The problem and solutions'. Brookings. Available at: <https://www.brookings.edu/articles/sextortion-the-problem-and-solutions/>

Mitchell, K.R., Purvis, A., Blake, C., Taylor, R.S. and Moore, L. (2025). Is a 'crisis of masculinity' evident in UK secondary student attitudes towards gender equality, gender stereotypes and sexual harassment? J Epidemiol Community Health. Available at: <https://eprints.gla.ac.uk/359592/1/359592.pdf>

National Crime Agency (NCA) (2025), 'National Crime Agency launches online campaign to tackle 'sextortion' among young teenage boys'. Available at: <https://www.nationalcrimeagency.gov.uk/news/national-crime-agency-launches-online-campaign-to-tackle-sextortion-among-young-teenage-boys?highlight=WyJzZXh0b3J0aW9uliwicmVwb3J0liwyMDI1XQ==>

National Youth Agency Digital Youth Work Standards (2025), Safeguarding standards for the youth sector. Available at: https://nya.org.uk/wp-content/uploads/2025/04/NYA_Safeguarding-Standards-for-the-Sector-April2025_update.pdf.pdf

NHS England (2023) 'One in five children and young people had a probable mental disorder in 2023'. Available at: <https://www.england.nhs.uk/2023/11/one-in-five-children-and-young-people-had-a-probable-mental-disorder-in-2023/>

NSPCC (2024), 'Online grooming crimes against children increase by 89% in six years'. Available at: <https://www.nspcc.org.uk/about-us/news-opinion/2024/online-grooming-crimes-increase/>

NSPCC Learning (2022), 'Behaviour management and codes of conduct'. Available at: <https://learning.nspcc.org.uk/research-resources/templates/behaviour-codes-adults-children>

Parliament (1989) Children Act 1989, c. 41. London: HMSO. Available at: <https://www.legislation.gov.uk/ukpga/1989/41/contents>

Parliament (2010) Equality Act 2010, c. 15. London: The Stationery Office. Available at: <https://www.legislation.gov.uk/ukpga/2010/15/contents>

Parliament (2014) Children and Families Act 2014, c. 6. London: The Stationery Office. Available at: <https://www.legislation.gov.uk/ukpga/2014/6/contents>

Parliament (2018) Data Protection Act 2018, c. 12. London: The Stationery Office. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents>

Pinterest (2022), Letter from Pinterest to Senior Coroner Andrew Walker. Available at: <https://www.judiciary.uk/wp-content/uploads/2022/10/2022-0315-Response-from-Pinterest.pdf>

Police Service of Northern Ireland (PSNI) (2024), 'Alexander McCartney sentenced to life imprisonment with a minimum tariff of 20 years'. Available at: <https://www.psni.police.uk/latest-news/alexander-mccartney-sentenced-life-imprisonment-minimum-tariff-20-years>

Ray, A. and Henry, N. (2025). Sextortion: A scoping review. Trauma, Violence, & Abuse, 26(1), pp.138-155. Available at: <https://journals.sagepub.com/doi/full/10.1177/15248380241277271>

Revenge Porn Helpline (2024) Revenge Porn Helpline 2024 Report. Available at: https://swgfl.org.uk/assets/documents/revenge-porn-helpline-2024-annual-report.pdf?_=1743672236

Sky News (2025), 'Fife school support worker who boasted of 'selling vapes to 11-year-olds' struck off'. Available at: <https://news.sky.com/story/fife-school-support-worker-who-boasted-of-selling-vapes-to-11-year-olds-struck-off-13376320>

The Sexual Exploitation Research and Policy Institute (SERP), 'Facing Reality: Addressing the role of pornography in the pandemic of violence against women and girls'. Available at: https://serp.ie/wp-content/uploads/2024/10/WA_SERP_Report_FINAL.pdf

UCL (2024), 'Social media algorithms amplify misogynistic content to teens'. Available at: <https://www.ucl.ac.uk/news/2024/feb/social-media-algorithms-amplify-misogynistic-content-teens>

Women's Aid (2023), Influencers Attitude and Attitudes. Available at: <https://www.womensaid.org.uk/wp-content/uploads/2023/12/CYP-Influencers-and-Attitudes-Report.pdf>

Contact Us



TELEPHONE

+44 (0)28 90 232 060



EMAIL

enquiries@ineqe.com



WEBSITE

www.ineqe.com

