Safe photos & Online posts

A practical guide for youth group leaders

For social media • websites • newsletters • promotional materials

THE GOLDEN RULE

Only share an image when you have a clear reason to use it, the right consent, and a safe way to publish it. If you are unsure, pause and check with your safeguarding lead or National VPC Safeguarding Manager.

Why this matters.

Photos and videos can be copied, saved, reshared or manipulated—including with AI tools. Images may be taken from public websites or social media and used without permission to expose personal information, or to create abusive material and even in some cases to blackmail individuals or organisations. Protecting images is part of safeguarding, not just a communications task.

Use this guide in three ways

- Before you post: use the quick checklist on the next page.
- Throughout the year: keep consent records, storage and published images under review.
- If something goes wrong: follow the response steps and contact the safeguarding lead promptly.

Important: This guide summarises practical points from the UK Safer Internet Centre's "Protecting your setting's images from AI manipulation and abuse". It does not replace your forces safeguarding, photography, data protection or online sharing policies.

1. Before you post: the quick checklist –

Use this every time you prepare a social post, website update or newsletter.

- Do we actually need an identifiable photo of a young person? Could a photo of the activity, artwork, equipment or venue tell the story instead?
- Have I checked the current consent record for this young person and this type of use?
- Have I considered the young person's own wishes and respected any "no photo" decision?
- Could the image or caption identify the young person, reveal sensitive information, or expose where they are or their regular routine?
- Can I use a less identifiable image—for example, taken from a distance, from behind, over the shoulder or without faces?
- Have I avoided full names and unnecessary personal details?
- Is the audience limited appropriately? Have I checked privacy and sharing settings?
- Have I removed image metadata (such as location, device details or timestamps) using the force approved method?
- Am I using an approved account and secure, approved storage?
- Would I be comfortable explaining this post to the young person, their parent/carer and our safeguarding

STOP IF YOU ARE NOT SURE

Do not publish yet. Check the consent record and ask the designated safeguarding lead (DSL) or named safeguarding person.

2. Choose the safest image that works

A useful starting question is: can we celebrate the activity without showing a child or young person's face?

Prefer, where practical

- Photos of crafts, displays, projects, equipment or the venue.
- Wide or distant shots, or images taken from behind or over the shoulder.
- Images that do not show identifiable faces or distinctive personal details.
- Lower-resolution images that are sufficient for the intended use.

Avoid or take extra care with

- Face-on close-ups, high-resolution portraits and images that are easy to reuse out of context.
- Full names, name badges, school or club identifiers, addresses or contact details.
- Backgrounds showing registers, paperwork, screens, whiteboards or other person information.
- Images showing distress, vulnerability, embarrassment, private care or sensitive circumstances.
- Live posts that reveal a young person's current location or regular schedule.

Remember

A private group is not a guarantee: members can still screenshot, download or forward images. Cropping, blurring or watermarking may reduce some risks but cannot guarantee that an image will not be misused.

3. Consent, privacy and secure handling

Consent: check it and keep it current

- Give parents/carers and young people clear information about where images may appear and the risks of online misuse or AI manipulation.
- Check the record before use. Consent for one channel or purpose does not automatically mean every use is covered.
- Where the young person is old enough and has capacity to decide, seek their agreement as well as parental/carer consent.
- Make consent information accessible, allow questions and explain how consent can be withdrawn.
- Review and renew consent regularly—for example, annually or at key transition points—following your force policy.

Privacy and publication

- Use the force approved accounts and platforms; do not publish youth group images from personal accounts unless policy explicitly allows it.
- Limit public visibility where possible. Consider whether a restricted audience can meet the purpose better than an open website or public social account.

- Avoid full names and unnecessary identifying details in captions, filenames, tags and image descriptions.
- Check the whole image and caption together. A photo that seems anonymous may become identifying when combined with a name, venue or event details.
- Do not assume that removing a name or turning off location services removes all identifying information.

Metadata, storage and retention

- Remove EXIF metadata before publication using an approved tool or process. Metadata can include location, timestamps and device details.
- Store original images in approved, access-controlled locations. Only people who need access should have it.
- Collect and keep only the images and information needed. Follow your force retention and deletion rules.
- Use suitable image resolution; avoid uploading originals or very high-resolution images when they are not needed.
- Consider whether approved protective tools, such as metadata removal or watermarking, are appropriate. These are additional safeguards, not a substitute for consent and careful image choice.

4. Keep checking after publication

Image safety is an ongoing responsibility—not a one-off check.

- Schedule and record image audits on the force website, social media and promotional materials. The source guidance suggests termly or twice-yearly reviews.
- Check that each image still has valid consent and remains appropriate for its context.
- Update or remove images that are outdated, no longer needed, no longer covered by consent, or create a safeguarding concern.
- Where appropriate, replace images of young people who are no longer members of the group.
- Include image security in volunteer/staff induction, refresher training, safeguarding procedures and communications/IT policies. It is included in the latest version of Safe to Operate Standards

Suggested routine

At the start of each term, check new consent changes and planned posts. At least termly or twice a year, record a review of published images and remove or update anything that is no longer appropriate.

5. If an image is misused, altered or used to threaten someone

Examples include an image being shared without permission, manipulated using AI, used to create sexual or humiliating content, or used in a threat or blackmail attempt.

Act promptly, calmly and without blame

Prioritise the young person's safety, dignity and emotional wellbeing. Do not blame them, promise secrecy, or try to investigate a serious incident yourself.

Protect and escalate: Tell the designated safeguarding lead (DSL) or named safeguarding person immediately. Follow the VPC safeguarding and incident-reporting procedures. If a child is at immediate risk of significant harm, call 999.

Contain exposure: Arrange for the original compromised image on your own website or social media to be made unavailable to the public as soon as possible. Request removal from other hosting sites/platforms where appropriate.

Preserve information safely: **Do not delete or further share communications** or relevant evidence. Store relevant material securely and seek advice from police and the DSL. **If sexual images of children are involved, do not download, copy, forward or take screenshots of the images**; seek immediate safeguarding/police advice about evidence handling.

Do not engage with blackmail: Do not respond to demands, negotiate or pay. Preserve the communications safely and report threats involving imagery to police through official force process, alongside internal safeguarding procedures.

Record and assess: Record the incident through the VPC normal process. With the DSL, assess the impact and risks to the young person and decide what notifications or further action are required.

Support the young person and family: Offer calm, non-judgemental support. The DSL should consider appropriate communication with parents/carers and support for affected staff, in line with safeguarding advice and the young person's circumstances.

Report and prevent recurrence: Use the relevant reporting routes below, review other published images and consent processes, and update policies, training or technical safeguards as needed.

Reporting and support links

Police — Report threats to publish sexual imagery of children or young people. Call 999 if a child is at immediate risk of significant harm.

Report Remove (under-18s) — A confidential UK service to help young people under 18 report sexual images or videos of themselves, including AI-generated images, and seek removal.

Stop NCII (adults 18+) — Helps adults prevent the sharing of intimate images without consent, including some AI-generated imagery.

Professionals Online Safety Helpline (POSH) — Advice for professionals working with children and young people on online safety concerns.

Stop It Now — Support and advice for adults concerned about child sexual abuse, including online abuse.

Useful links: Report Remove | Stop NCII | Professionals Online Safety Helpline | Stop It Now | UK Safer Internet Centre image guidance

6. Our youth group: local contacts and actions

This is a template that could be used to record force process and document official permissions and responsibilities. Complete this page before sharing the guide with volunteers.

Unit	_____
Designated safeguarding lead / named person	_____
Safeguarding contact details	_____
Deputy / alternative contact	_____
Approved photo storage / account guidance	_____

Our agreed routine

- Before publishing: check consent, image content, caption, audience and metadata.
- When consent changes: update the record and review existing published images.

Image audit date / frequency: _____

Where to record a concern or incident: _____

Who is authorised to publish: _____

x