



Online Safety, Social Media and Images Policy

FACE – Family and Community Enterprise | Registered charity 1179629 | Working as FAM

Head office: Central Buildings, Richmond Terrace, Blackburn, BB1 7AP | Applies at head office and all FAM outreach sites

REFERENCE	VERSION	OWNER	REVIEW
FAM-SG-03	1.0 (September 2026)	Designated Safeguarding Lead	Annually

Status: approved by the Board of Trustees on 10 September 2026.

Our commitment

FAM uses digital tools, social media and images to connect with young people and share the difference our work makes, but never at the expense of their safety or privacy. All contact with young people happens through organisational accounts, and no image is taken or used without the right consent. Anyone under 18 is never named or located in images we publish.

1 Purpose and scope

- 1.1** This policy sets out how FACE – Family and Community Enterprise (registered charity 1179629), working as FAM, keeps young people and staff safe online, uses social media, and takes and uses photographs and films. It applies to trustees, staff, volunteers, sessional workers and anyone taking images at FAM activities, including partners and freelance photographers.
- 1.2** It covers FAM's own social media accounts and website, messaging with young people, online sessions, personal use of social media where it touches on FAM, and images and recordings of any kind. It should be read with 01 Safeguarding Children and Young People Policy. Relevant law includes the Online Safety Act 2023, UK GDPR and the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025).

2 Key rules at a glance

- Contact young people **only through FAM accounts and FAM devices** — never personal numbers or personal social media.
- **Never** put a name alongside an image of a young person under 18.
- **Never** share details that could identify where a young person lives, goes to school or can be found.

- No photograph or film without the right consent recorded first.
- Report any online safety concern to the DSL the same day.
- Never view, save, copy or forward an indecent image of a child, even to report it.

3 Photography and filming

Consent

Age	Consent needed
Under 16	Written consent from a parent or carer and the young person's own agreement. If the young person does not want to be photographed, we respect that, even if a parent has consented.
16 and 17	The young person's own written consent. We involve parents or carers where appropriate.
18 and over	The person's own written consent.

3.1 Consent forms say clearly how images may be used (for example: internal records only, funder reports, website, social media, printed materials, press) and let people choose each use separately. Consent lasts for the current programme year, or until withdrawn, and is renewed each year.

3.2 People can withdraw consent at any time by telling any member of staff. We will then stop any new use and remove images from our own website and social media the same day. We cannot recall printed materials already distributed, and we explain this when consent is given.

Extra care

- Some young people must **never** be photographed or filmed for publication, or only in ways that cannot identify them. This includes looked-after children where the local authority has not agreed, young people at risk of exploitation or in contact with exploiters, anyone in a family subject to a court order or fleeing domestic abuse, and asylum-seeking or refugee young people where publicity could put them or their family at risk. Workers check the 'no photo' list before any session.
- Young people new to the UK may not fully understand what social media publication means. Explain consent in plain language, using a professional interpreter where needed.
- Make sure everyone is appropriately dressed. Do not photograph young people changing, swimming or in positions that could be misread. Avoid close-ups of individual children at sport and swimming events.
- Use group shots of the activity where possible.

Using and publishing images

- **No names with images of any young person we support, whatever their age** — no first names, surnames, nicknames or tags in captions, file names shared publicly, or alt text.

- **No identifying location details** — do not show school uniforms or badges, street signs, house numbers, car registrations or distinctive landmarks near where young people live. Post about trips and events after they have happened, not live.
- Turn off location tagging and remove location data from image files before publishing.
- For over-18s, a first name may be used only with their specific consent.
- Case studies use a changed name and no photo, unless separate specific consent has been given.

Devices and storage

- 3.3** Images are taken only on FAM devices. Personal phones and cameras must not be used, except in an emergency agreed with the session lead, in which case images are transferred to FAM storage and deleted from the personal device the same day. Images are stored on FAM's secure shared drive with restricted access, and deleted in line with 15 Records Management and Retention Policy.

Parents, visitors and the media

- 3.4** Parents and carers may take images of their own child at public events for personal use only, and we ask them not to post images of other children online. At other sessions, visitors may not take images. Press and freelance photographers must be briefed on this policy, supervised at all times, and only photograph young people who have given consent.

4 FAM's social media and website

- FAM's social media accounts are managed by the Operations Lead or staff they authorise. Passwords are held securely, use multi-factor authentication, and are changed when anyone with access leaves.
- Posts must be accurate, respectful and in line with our purposes. FAM never supports or opposes any political party or candidate. Any campaigning post must link clearly to our purposes and be agreed by the Operations Lead first.
- Complaints received on social media are moved to our complaints process (see 16 Complaints Policy).
- Harmful, abusive or discriminatory comments are hidden or removed, screenshotted for our records if needed, and reported to the platform. Safeguarding-related comments are reported to the DSL.
- We do not 'follow' or 'friend' individual young people from FAM accounts.

5 Personal use of social media

- Staff and volunteers must **not** accept or send friend or follow requests to young people who take part in FAM activities, or to their families where this could blur boundaries, while that working relationship exists. This includes young people aged 18 to 25 on our programmes.
- If a young person contacts you on a personal account, do not reply from that account. Tell your line manager, and respond, if needed, through a FAM account.

- Do not post anything about young people, their families, or sessions on personal accounts, including photos, comments or 'check-ins'.
- Do not post anything that could bring FAM into disrepute or breach 04 Code of Conduct and Professional Boundaries (Staff and Volunteers) or 11 Equality, Diversity and Inclusion Policy.
- If you have a pre-existing relationship with a young person or family (for example a relative or neighbour), tell your line manager so it can be recorded.

6 Messaging and contact with young people

- Use **only** FAM-issued phones, FAM email addresses and FAM-approved messaging or social media accounts.
- Group messages are preferred to one-to-one messages. Where one-to-one contact is needed (for example in mentoring), it must be for a clear work purpose, and messages must be kept and be available to your line manager and the DSL.
- Keep messages short, professional and about FAM activities. No kisses, emojis that could be misread, private jokes or late-night contact.
- Only message during agreed working hours unless there is an urgent safety reason, which must be recorded.
- Under-16s are added to group chats only with parent or carer consent. Group chats are set up by FAM, have at least two staff members as administrators, and have clear ground rules.
- Never share personal contact details with young people, and never ask for young people's personal images.
- If a young person sends something worrying, such as a disclosure, a threat of self-harm or an inappropriate image, do not delete it, and tell the DSL immediately. If it may be an indecent image, do not look at it again, forward or copy it.

7 Online sessions

- Use a FAM account on an approved platform. Meeting links are sent only to registered participants or through their parents or carers for under-16s, and waiting rooms or passwords are used.
- At least two DBS-checked staff or volunteers are present in every online session with under-18s. One-to-one online sessions are only held where agreed in advance with a manager, recorded in the session log, and with parent or carer consent for under-16s.
- Staff join from a neutral, private setting with a plain or blurred background, and are appropriately dressed. Young people are asked to join from a shared space in their home where possible, not their bedroom.
- Sessions are not recorded unless there is a clear reason, participants and (for under-16s) parents or carers have agreed in advance, and the recording is stored and deleted in line with our retention policy.
- Ground rules (respect, cameras, chat, no screenshots) are agreed at the start. Staff control muting, removal and screen-sharing.

8 Keeping young people safe online

- 8.1** We help young people understand online risks, including grooming, sextortion, scams, misinformation, harmful content and online radicalisation, and we know that young people new to the UK may be targeted online. We teach them how to block and report, and who to talk to. Where FAM provides internet access or devices, we use appropriate filtering and supervision, and young people agree to an acceptable use agreement.

Nude and semi-nude images

- 8.2** If a young person under 18 shares or is asked to share nude or semi-nude images, or tells you about one, tell the DSL immediately. Do not view, copy, print, share or delete the image, and do not ask the young person to send it to you. The DSL will follow local authority and police guidance. The DSL can also help the young person use reporting services to get images removed.

9 Responding to concerns

- 9.1** Any concern about online harm, misuse of images, or inappropriate contact between an adult and a young person is reported to the DSL the same day, following the procedure in 01 Safeguarding Children and Young People Policy or 02 Safeguarding Adults at Risk Policy. Breaches of this policy by staff or volunteers may lead to action under 19 Grievance and Disciplinary Procedure or 18 Volunteer Policy. Loss of a device or images is a data breach and must be reported to the Data Protection Lead at once, under 13 Data Protection Policy.

10 Roles and responsibilities

Role	Responsibilities
Board of trustees	Approves this policy and makes sure it is followed.
Designated Safeguarding Lead	Owens this policy; handles online safety concerns; keeps the 'no photo' list up to date with the Operations Lead.
Operations Lead	Manages FAM's social media and website accounts, devices and access.
Data Protection Lead	Advises on consent records, storage and data breaches.
Session leads	Check consent and the 'no photo' list before any images are taken; run online sessions safely.
All staff and volunteers	Follow this policy and report concerns the same day.

11 How this policy supports our focus

- Every FAM programme builds young people's digital and AI confidence. This policy sets the safe, honest way we do that, including sensible use of AI tools for learning and job applications.

- Images and online contact are managed with extra care for girls and young women, young people with SEND and young people new to the UK, whose safety online can carry additional risks.

12 Related policies

- 01 Safeguarding Children and Young People Policy
- 02 Safeguarding Adults at Risk Policy
- 04 Code of Conduct and Professional Boundaries (Staff and Volunteers)
- 07 Activities, Trips and Transport Policy
- 11 Equality, Diversity and Inclusion Policy
- 12 Anti-Bullying and Harassment Policy
- 13 Data Protection Policy
- 14 Privacy Notice (Participants, Families and Supporters)
- 15 Records Management and Retention Policy
- 16 Complaints Policy

Approval record

Approved by the Board of Trustees on	10 th Sep 2026
Signed (Chair of Trustees)	
Next review due	31st July 2027
Version history	1.0, September 2026. New policy; replaces any earlier FAM or FACE version.