

Guide for Charities Targeted by the Far Right

imix

Contents

- Principles to Hold
- Rapid Response (First 72 Hours)
- Managing a Protest
- Media Strategy
- Social and Digital Hygiene
- Staff Wellbeing and Duty of Care
- Funders, Regulators, and Allies
- Templates and Checklists
- After the Peak: Recovery and Rebuild
- Minimal Crisis Plan (One-Pager to Copy)
- 5 Ways to Show Solidarity Safely

1. Principles to Hold

- Safety first. Physical safety and safeguarding is more important than media/perception. Ensure all your staff, volunteers and clients are safe, know what to do if they personally become targets and how they can look after their own mental health.
- De-escalate. Don't feed the outrage machine; reduce oxygen and vectors for harm. This includes on social media, do not amplify the hate even if you are criticising it.
- In communications, be factual, brief, calm. Correct misinformation once in owned spaces; avoid back-and-forth with agitators particularly online and in public spaces.
- Protect people's data. Minimise personal identifiers everywhere. This could include removing the team page from your website.
- Solidarity, not isolation. Ask for help; coordinate with allies. Remember, you are not alone.



2. Rapid Response (First 72 Hours)

A. Situation Room

- Set up a small incident team including a leader, ops/safeguarding, comms and legal liaison.
- Create a single live log (time-stamped) of incidents, decisions, and evidence. Document everything including screenshots, URLs and emails.

B. Security & Safeguarding

- Email: Switch to central inboxes (e.g., info@) for public contact; remove direct staff emails from website. Set up a dedicated threats@ inbox and auto-forward filters.
- Website: Triage the website, remove or redact staff bios, trustee lists, and sensitive PDFs; review resources through a hostile-read lens; add clear explainers of what you do. This explainer could also be shared on social media if necessary.
- Social: Lock down personal accounts ensuring privacy settings are activated, remove work links on private accounts. Keep organisation social media accounts live to prevent impersonation, but pause posting on high-risk platforms (esp. X/Twitter) while monitoring.
- Events/Zoom: Hide links behind registration and approve manually; disable auto-send of meeting links; consider postponement of sensitive sessions.
- Physical: PO box or mail redirection; review entry controls; brief reception/FOH; prepare a “lockdown light” plan for protest days.

C. Threat Intake and Reporting

- Triage incoming emails/messages into different sections such as
- Threat / Harassment / Inquiry.
- Report credible threats to police; keep incident numbers; consider True Vision hate crime reporting.
- Escalate doxxing to platform abuse teams (harassment/privacy categories); flag content involving minors with higher priority.

D. Legal and Regulatory

- Seek initial advice around media, defamation and harassment concerns. Record potential IPSO (Independent Press Standards for Organisations) breaches for later complaints.
- Where risk is credible, request temporary suppression of trustee/staff details with Charity Commission; add a safeguarding note in correspondence.

E. Stakeholder Comms (Quiet, Targeted)

- Internal: Brief staff and volunteers on communications telling them not to engage and route all media enquiries to the comms. lead. Ensure everyone knows how to secure personal profiles and handle calls.
- Funders and Key Partners: Provide a one-pager update and ask for crisis-comms/legal support if needed.
- Service Partners (if relevant): Share a short factual note, a link to your statement, and practical safety steps.

F. Public Statement (Only if needed)

- Keep concise; correct specific falsehoods, avoid repeating smears.
- Emphasise safeguarding, mission, and support available for affected communities.
- Use “spokesperson” attribution; avoid naming individuals.

3. Managing a Far Right / Anti-Migrant Protest

- **Intel:** Confirm date/time/location with local authority/police; monitor organiser credibility and traction.
- **Site Safety:** Coordinate with venue/local authority; brief staff on avoidance routes; discourage counter-mobilisation by staff; signpost to community stewards if applicable. Ensure no-one feels compelled to attend a counter demonstration on the same day particularly if they are worried about becoming a specific target.
- **On the Day:** Keep premises access-controlled; designate an offsite comms base; log incidents and capture evidence; no doorstep comments—use pre-planned written lines only.
- **After:** Debrief with police/local authority; update staff; offer wellbeing support.
- **Monitor:** For potential future protests in your area and stay informed on local developments, such as the opening of a new accommodation site.



4. Media Strategy

- **Reactive only comms and media during peak of the attack:** A calm holding line on request; no proactive unless/until threat subsides.
- **After the storm:** Consider a reflective piece on the **impact of misinformation** on your organisation, centring your beneficiaries, and/or targeted outreach to sympathetic titles/audiences (e.g., faith/community media where alignment is strong). Ensure audiences understand the ongoing impact of threats and protests on your service delivery.
- **Photo/language hygiene:** Avoid imagery/language that can be twisted; offer journalists guidelines. Again seek to quell the hate and mis/disinformation while promoting the crucial work of your organisation.

Holding line (example):

“We provide [clear description of service]. Recent claims circulating online are false. Our priority is the safety and wellbeing of staff and our community. We are working with partners and authorities and won’t be commenting further while they address abusive content.”



5. Social and Digital Hygiene

- Do **not** block agitators in-flight as this can lead to escalation. Use mute/report functions; keep evidence.
- Register close variants of your handles to prevent spoofing.
- Pause posting on high-risk channels particularly on X (Twitter); keep monitoring; resume with normal content once safe. Consider which social media platforms work best for your organisation and audiences.
- Create a “reporting pack” for allies: link-free instructions for reporting posts and why public pile-ons/quote-tweets can amplify harm.



6. Staff Wellbeing and Duty of Care

- Offer EAP (Employee Assistance Programme) /therapy signposts; normalise switching off and handing over. Create a work culture which prioritises boundaries and self-care.
- Rotate inbox duty; cap after-hours exposure; provide template replies so individuals don't draft alone.
- If an individual is doxxed/named, assign a buddy and offer home security guidance (e.g. remove address from public registers where possible).



7. Funders, Regulators, and Allies

- Proactively update funders; some can release emergency comms/legal funds.
- Coordinate with sector bodies for rapid advice, sample lines, and early-warning alerts about hostile coverage.
- Keep local education unions, councils, and community groups in the loop where your work touches schools or public services.



8. Templates and Checklists

A. Inbox Auto-Reply (Threats@)

Subject: We've received your message

Thanks for your email. If your message contains a threat or abusive content, it has been logged and will be reported where appropriate. For legitimate enquiries, contact us at [central inbox] and we'll respond as soon as we can.

B. Staff Brief (Slack/Email)

- Do not respond to hostile messages; forward screenshots.
- Switch personal social media accounts to private; remove employer and location.
- Route media to **press@**; use “spokesperson” only rather than named members of staff.
- If you feel unsafe, tell your manager immediately and step back from public-facing tasks.

C. Partner Note (Schools/Delivery Partners)

We're aware of misinformation circulating online about our work. We provide [clear description]. Safeguarding is central to everything we do. Please direct any enquiries to [central inbox] and do not engage with hostile accounts. Here are platform reporting links and safety tips for your teams.

D. Protest Day Checklist

- ☐ Confirm timings and routes with local authority/police
- ☐ Premises access controls tested; visitor policy briefed
- ☐ Offsite comms base set; emergency contacts printed
- ☐ Evidence capture lead assigned; shared folder ready
- ☐ Staff rota avoids unnecessary travel through protest zone

E. Website “What We Do” Explainer (150–200 words)

- Plain-English description; safeguarding commitments; links to policies; contact via central inbox only.

9. After the Peak: Recovery & Rebuild

- **Review statement:** Update or retire; archive a final version for transparency.
- **Proactive myth-resistant content:** Short explainer posts; beneficiary stories; third-party validators (e.g., schools, local leaders, faith partners) once safe. Rather than referring back to hateful or inaccurate content, be proactive and positive in communications about the work of your organisation.
- **Learning review:** What triggered attention? Which assets were vulnerable? What helped staff most? Does anything need to change in public communications moving forwards as a result?
- **Update your crisis plan:** Ensure playbooks and contacts are kept up-to-date.

10. Minimal Crisis Plan (One-Pager to Copy)

- 1. Team and Roles:** Incident lead; ops/safeguarding; comms; legal; admin.
- 2. Contacts:** Police 101/999; local authority lead; platform escalation forms; legal; funders.
- 3. Decision Rules:** Safety first; do not engage in live debates; single public statement for website and social media channels
- 4. Channels:** Pause high-risk channels; monitor; centralise inbox.
- 5. Data Security:** Remove personal identifiers; review PDFs; redact addresses.
- 6. Staff Care:** Rotas; EAP signpost; boundaries; mental health support and self care; buddy system; escalation thresholds.
- 7. Templates:** Holding lines; ally reporting pack; partner note; auto-replies.
- 8. Protest Protocol:** Intel → safety → evidence → debrief.

Five Ways to Show Solidarity Safely

When charities are targeted by far-right campaigns, allies want to show support. Public pile-ons or amplified posts can make things worse. Here are safe, effective ways to stand in solidarity without causing harm.

1. Reach Out Privately

- Send a supportive email or message directly to the organisation.
- Check in again after a few days—sustained support matters.
- Avoid public tagging, which can attract trolls.

2. Report, Don't Amplify

- Use platform tools to report abusive or misleading content.
- Do **not** quote-tweet or publicly argue with agitators—it spreads their content further.
- Ask colleagues to do the same; strength in numbers helps takedowns.

3. Offer Practical Help

- Review or proof draft statements.
- Share trusted media contacts.
- Offer to help monitor inboxes or social channels for a few hours.

4. Back Up Behind the Scenes

- Funders: offer emergency comms, quick-release grants or legal support.
- Partner orgs: lend staff capacity for admin, safeguarding, or press handling.
- Share safety tips or digital security guides discreetly.

5. Support Staff Wellbeing

- Remind colleagues it's okay to log off and step back.
- Point to counselling or peer support services.
- Normalise rest and rotation of stressful tasks.

Quick Solidarity Checklist

- Send private message of support
- Report harmful posts (don't share)
- Offer capacity (comms, legal, safeguarding)
- Connect with funders/partners for back-up
- Share wellbeing resources

Remember: Solidarity works best in private messages, reporting hostile content, offering real support, and helping behind the scenes —not in public pile-ons.



Telling the human story of migration

Find us on



@imix_uk



@human_journeys

Email us at

media@imix.org.uk