

**HATE**  
**HOPE**  
**HATE**

# KEEPING SAFE ONLINE



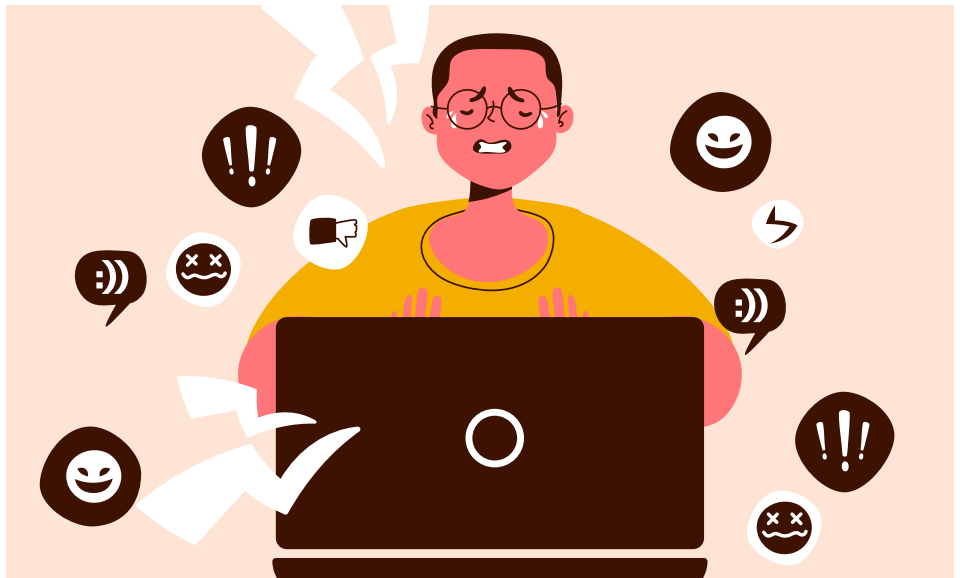
**A GUIDE FOR ORGANISATIONS AND INDIVIDUALS  
LOOKING TO IMPROVE DIGITAL SECURITY IN LIGHT OF THE  
ONLINE FAR-RIGHT THREAT**

Recent far-right activity in temporary accommodation has meant increased scrutiny of organisations in the sector, including on social media. In this resource, there are a number of practical tips on how to improve online safety preventatively and how to respond to breaches of security. HOPE not hate is not an organisation dedicated to digital security, but we have collated best practice from a variety of sources here.

**Caveat:** You might not need to implement every recommendation in the resource. Safety is highly contextual, and some people will want or require a higher level of security than others due to their work, needs and previous experience. The aim of this resource is to provide people with as much information as possible so they can make informed decisions.

## WHAT DOES THE MIGRATION SECTOR THINK?

Of the organisations surveyed by Hope Not Hate and Refugee Action in March 2023, **over half** said that they had **experienced far-right activity in the past 12 months**. A number of respondents explicitly mentioned online abuse on both organisational and individual social media accounts, as well as asylum seekers reporting abusive messages and abusive comments on local news websites and social media.



## FIND YOUR ONLINE SAFETY COMPROMISE

Lowest risk of negative interactions, but reduced stakeholder reach

Lowered risk, maintaining usability and engagement

Highest risk of negative interactions and compromise of safety

*Maximal online security*

*Minimal online security*

## GENERAL ONLINE SAFETY

The below tips are general good practice for being online, and could be used by anyone to keep safe. It is likely that any information placed on the internet or social media will be considered a public disclosure in legal proceedings. People should consider the security of both organisational and personal accounts.

- **Passwords:** To avoid the threat of hacking, we suggest you have a different password for every online account, especially social media accounts. Password vaults, which are apps that securely store your various passwords, are helpful for this.
- **Two-factor authentication:** Using two-factor authentication, where you need to use more than one device to log into an account, makes your accounts less vulnerable to hacking. For example, you could receive a text message or email to confirm it's actually you logging into the account. If you receive these messages but have not tried to log in, someone else might be trying to access your account.
- **Check for hacks:** the website [Have I been pwned?](#) helps you to check whether your email address and passwords have been breached online. You should change all passwords associated with the email account if it has been breached.



## PRIVACY ON SOCIAL MEDIA

People engage with social media in different ways, and some people are comfortable having information shared publicly that others will be more cautious about.

However, consider the following if you are concerned about online security:



- 1. Limit location information** - people can figure out patterns of where you live, work or spend time from location tagging settings on social media - which can be switched off - or from recognisable features in the background of photos. If you are posting whilst at a location or live streaming, anyone able to view that post will know where you are. Consider avoiding public posts which make the locations of the office and people's homes clear, and only posting tagged locations after you have left.
- 2. Privacy settings for posts and tagged photos** - ensure that what you post on your own profile is only visible to the audience you want. For example, you can choose for content to be seen by anyone, friends of friends or only your friends. Tagging people in photos or allowing yourself to be tagged on profiles, groups and pages means that people can access posts about you through other people's profiles, which may be less secure than yours. Privacy settings change from time to time on platforms, so it can be helpful to regularly check for changes to your profile(s).
- 3. Limit who can access your profile** - your privacy settings do not guarantee that anything you post online will remain private. For example, a Facebook "friend" may pass your comments on. Consider whether you might benefit from having separate accounts for your personal social media use with more restrictive privacy settings if you have to be more public for work purposes.
- 4. Audit friends and followers** - it can be helpful for organisations and individuals who are at higher risk of trolling and online abuse to regularly check through follower lists. If a follower/subscriber/friend seems suspicious or does not align with yours or your organisation's values, consider blocking or removing them.

## SECURITY TIPS FOR HOSTING AN EVENT ON ZOOM

It is important for you to consider how to strike a balance between security needs and the needs of the event. Some of these tips will not be feasible if you want to use certain functions of Zoom, and they might be too precautionous if you are not sending out public invitations to your event.

- If you are concerned about infiltrators taking over the meeting, use the **webinar function**, which means that only the speaking panel can speak and show video. You have to sign up for webinars with a name and email, so you will have a list of participants.
- In webinar mode, it is possible to **close the sign up list** a few hours before the event so that you can check the names of sign-ups to exclude suspicious names.
- Ensure **screen sharing is set to “host only”** to ensure participants do not share harmful content or derail the event. If someone else needs to share their screen, the host can share permission during the call.
- It can be helpful to have a **moderator** (or two!) if you suspect that your event may be at risk. The role of a moderator is to monitor the meeting including the chat, screen sharing and breakout rooms. They can also block people quickly during the call if needed.
- You may want to **“lock” the call** after it’s started or a few minutes in to avoid lots of people joining the call halfway through, which can be derailing. This can be particularly helpful if you do not have a moderator.
- In some cases, calls are recorded or participants could be recording their screens. It is best to **avoid directly quoting harmful material** as this can be clipped and misedited to make it appear as though you are saying it. If in doubt, paraphrase the harmful language.
- **Keep alert to the chat box** in the last two minutes of the conversation, this is when spamming and abuse are most common. If you have had issues with spamming previously, you might consider turning off the chat altogether, although obviously this will affect engagement with your event.

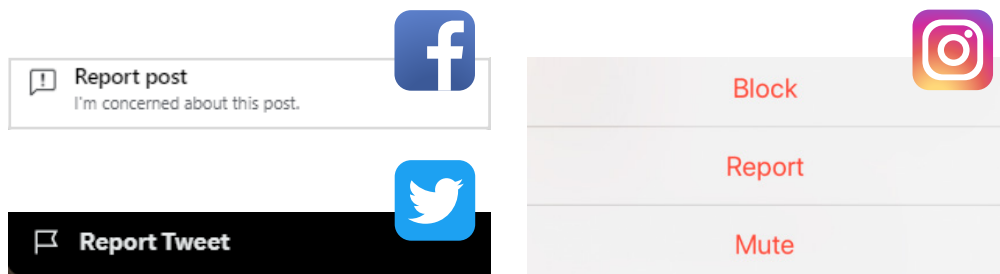


## TROLLS

Engaging with trolls (often anonymous online abusers) is not advisable. Choosing to respond (either by replying to individual comments or by saying that you are being targeted) gives trolls the oxygen they seek, and they will just come back for more. Other potential trolls will spot a ‘vulnerable’ target, and join the fray. If any comments or posts are particularly hateful or distressing, take screenshots and save them on your computer, saving the time, date and sender in case you need to report them through internal safeguarding procedures or if you choose to report trolling as harassment or a hate crime, if it qualifies. You may also want to block accounts and report comments. If the account being trolled is an organisational one, contact your HR or communications officer to receive further guidance.

## REPORTING

Reporting is the main way that social media companies regulate content. Without content being reported by users, it very rarely gets removed. For that reason, it can be helpful to report anything you see online that violates the guidelines of the social network or even, in extreme cases, appears to break the law. When reporting an account or comment, the more detail you can give, the better. For example, when reporting an account you can often select posts or tweets which violate guidelines. The person being reported is not notified that you have reported them unless they receive a warning or changes are made to the account. You will never be named as the person who made the report. [This is a good guide](#) to reporting on different social media platforms. You are usually informed by the platform if your report is unsuccessful, in which case you might choose to block the account you reported so you no longer see their content. Since you might lose access to the account, you should take any screenshots you might need before making a report. You can use the screenshots internally as evidence collection for internal use or for possible criminal proceedings, if it meets thresholds for hate crime reporting.



Examples of reporting buttons on Facebook, Twitter and Instagram

## SHOULD I POST ABOUT MY NEGATIVE EXPERIENCE?

Receiving online abuse, whether on a personal or organisational account, can be scary and exhausting. The main thing to remember is that in most cases, the onslaught dies down eventually, and in the meantime it is important to consider how you can look after your wellbeing, and find support for and from colleagues. Even if the account receiving abuse is not named, the person who checks it most frequently is still likely to be affected.

Sometimes, people want to speak up on their abuse in defiance of trolls. Sharing online can often result in further attention landing on a person, which can end up defeating the point of the exercise. Private, closed groups on secure social media apps like WhatsApp or Signal are best for sharing safely with a wider community. It might be worth reaching out to other local activist groups, even if they are in a different sector. People can offer solidarity and share their experiences of trolling or abuse and how they followed up. Remember that the context and circumstances will be different for different people, so there will not be a one-size-fits-all solution.



### Hotels Housing Illegals (The Last Stand)

+ Invite

Discussion Featured People Media Files Reels

Q ...

An example of a Facebook community group where anti-migrant far-right activity is common.

## DOXXING

Although rare, there have been cases of people supporting asylum seekers having their personal information (such as their workplace or home address, personal social media images or personal backgrounds) released publicly on the internet without their consent. [This guide from Equality Labs](#) is a particularly good source of advice as it is geared towards activists. Following the steps to improve your security preventatively is the ideal scenario, but there is also helpful information on what to do if you have been doxxed.

## ONLINE COMMUNITY GROUPS

1. Before joining a “group” or affiliating yourself with other organisations, campaigns or individuals, check that its views are compatible with the values of you or your organisation.
2. Some people use pseudonyms online for greater safety, or to embolden their online behaviour. Consider whether being identifiable will put you at risk, or emphasise your honesty and accountability to the community. Using anonymous accounts does not guarantee safety, because there can still be other identifying details on a profile. Following and interacting with anonymous accounts can be risky, too.
3. Ideally, community groups should have more than one admin whose job it is to moderate conversation in the group and ensure posts meet both the platform’s community guidelines and the rules decided by the group. If a community group has become toxic, consider asking the admin to rewrite the group rules and publicise this.

Groups on social networks such as Facebook, WhatsApp and NextDoor provide opportunities for members of a community to share information with each other and compare views and experiences. However, we have also seen groups be created or used to scrutinise and criticise behaviour of asylum seekers and other marginalised members of the community. Unlike the media, reports and claims made on community groups have not been fact-checked, edited or vetted in any way. This allows for more authentic communication, but also for speculative claims and, in the worst cases, hate speech to be published online.



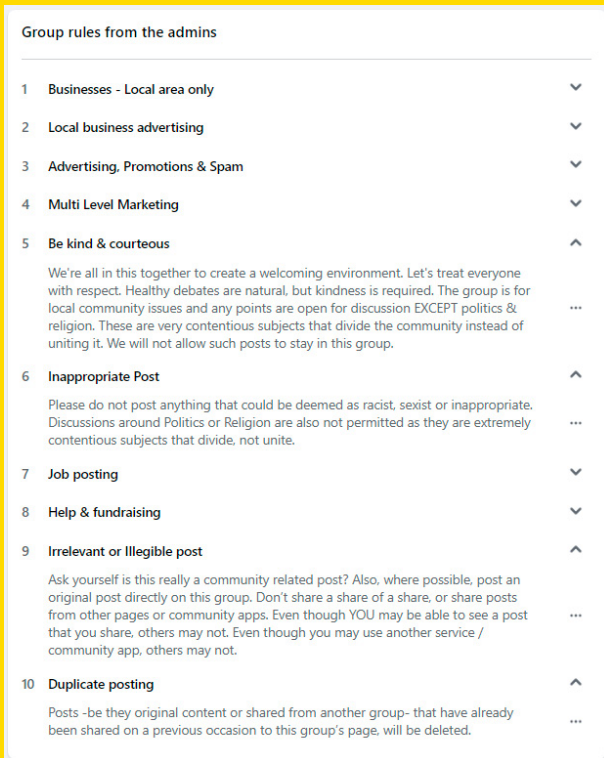


## GOOD PRINCIPLES FOR RULES ON ONLINE COMMUNITY GROUPS

Facebook has the option to add rules to a group which clearly display the purposes, joining requirements and guidelines for how the group should be run. Group admins should consider the purpose of the group and decide on rules which, if broken, result in being warned or eventually removed from the group. The rules can be tagged in comments, which can be used to identify users who are breaking rules. The following are ideas of what to include, which should be put in your own words:

- Kindness and courtesy for all members of the group
- Any user degrading comments about race, religion, culture, sexual orientation, gender or identity will be banned from the group
- If the group is for a particular section of the community (e.g. a specific geographic area or a specific identity), it needs to be mentioned clearly. There should also be consequences of what will happen if admins suspect a group member does not conform to the rule
- What type of content should be posted on the group, as well as consequences for inappropriate content being posted
- Encourage use of the search function so posters can see if the same or a similar topic has already been discussed in the group
- Make it every group member's responsibility to report and monitor group content, including alerting admins when rules are seen to have been broken

An example of community group rules on Facebook which have been edited by admins - relevant rules have been expanded.



The screenshot shows a list of 10 group rules from the admins. Each rule is numbered and has a corresponding icon (chevron down or up) on the right. Some rules have a three-dot menu icon next to them. The rules are:

Group rules from the admins	
1	Businesses - Local area only
2	Local business advertising
3	Advertising, Promotions & Spam
4	Multi Level Marketing
5	Be kind & courteous We're all in this together to create a welcoming environment. Let's treat everyone with respect. Healthy debates are natural, but kindness is required. The group is for local community issues and any points are open for discussion EXCEPT politics & religion. These are very contentious subjects that divide the community instead of uniting it. We will not allow such posts to stay in this group.
6	Inappropriate Post Please do not post anything that could be deemed as racist, sexist or inappropriate. Discussions around Politics or Religion are also not permitted as they are extremely contentious subjects that divide, not unite.
7	Job posting
8	Help & fundraising
9	Irrelevant or Illegible post Ask yourself is this really a community related post? Also, where possible, post an original post directly on this group. Don't share a share of a share, or share posts from other pages or community apps. Even though YOU may be able to see a post that you share, others may not. Even though you may use another service / community app, others may not.
10	Duplicate posting Posts - be they original content or shared from another group- that have already been shared on a previous occasion to this group's page, will be deleted.

## ONLINE INFORMATION ABOUT ASYLUM ACCOMMODATION

Using websites or social media accounts for publicity can be helpful for organisations with volunteers and stakeholders who enjoy keeping up-to-date with the latest activity, however these can also be used in bad faith by the far-right. Sometimes it will be beyond your control that the address of an accommodation site is widely available. However, where possible, try not to make too much information about locations of asylum accommodation and events hosted there publicly available. For example, if there is no clear need for the times of visits to accommodation from organisations to be posted online, consider removing this. Of course posting things online can be helpful or necessary for organisations, so you will need to consider the trade-off between easily accessible information and security. If you see information online that could compromise accommodation sites, for example council or public service websites listing them, consider contacting them and asking for the information to be taken down.



Credit: [The Guardian](#)



## ONLINE SAFETY FOR RESIDENTS OF ACCOMMODATION

This information could be helpful to share with residents of accommodation or other service users you work with. Note that the tone of this is really important - we don't want people to become afraid of using basic services which could be a lifeline for them, but given our knowledge of what can be weaponised by communities and the far-right it is important to make sure service users are kept safe and feel secure.

- Be aware of who is around when you make video calls or voice calls. Members of the community might be sensitive to who is being captured on video, even if it is in the background of a call. This is particularly the case around schools, playgrounds, shops etc.
- If you are nervous about making a call in a public area, it might be better to wait until you are somewhere more private or around people who don't mind being the background of your call.
- Think carefully about whether you want to be a part of a community group on social media. It could be helpful to understand the people and priorities in the local area, but it may also contain distressing content about the hotel or articles shared which are negative. In-person groups, where people can get to know you as a person, can be better for building links in the community.
- Be careful of what sort of intentions non-residents have when it comes to information about the hotel. Of course it's completely normal to share information about your situation, and it can be helpful to talk. However, it might be helpful to first establish that the conversation is private. We have seen reports of conversations with residents of accommodation unknowingly being shared on social media and used against them, for example residents explaining to a local where the people staying in the hotel have come from and whether there are any women or children there.



## SHARE YOUR STRENGTH AND RESILIENCE WITH US!

HOPE not hate are always looking to champion communities who put up a fight against harmful far-right narratives. If you would like to share news about acts of solidarity happening in your community and be the hope for someone else, email us at [towns@hopenothate.org.uk](mailto:towns@hopenothate.org.uk)



HOPE not hate Ltd  
Registered office:  
Suite 1, 7th Floor, 50 Broadway,  
London SW1H 0BL, UK