Online Group Chats

Mattermost, Signal, WhatsApp and Telegram - how to choose! Set up and run a secure and effective XR group chat.

- Quick comparison of the chat apps

- Choosing a messaging app for your XR group

- How to set up and run effective group chats

  - When setting up the group chat make sure you

  - Tips and recommendations for moderating a group chat

- Keeping Group Chats secure

  - Comparing Security of Signal, Telegram and WhatsApp

  - Guidelines to keep the Group Chats as secure as possible

  - Hide your phone number from others using Telegram

  - Telegram: How to remove spammers

- Chat Etiquette for XR Group Chats

- Online Behaviour Guide

- How to find information in a group chat

Quick comparison of the chat apps

Comparison of the drawbacks and benefits of Mattermost, WhatsApp, Telegram, and Signal. For more detail see Choosing a messaging app for your XR group in the "Online Tools for Communicating with Other Rebels" book.

Here is the summary from that chapter:

	Whats-App	Telegram	Matter-most	Signal
Security	★★	★★	★★★★	★★★★★
Accessibility	★★★	★★★	★★★★★	★★
Features	★★★	★★★	★★★★★	★★★
Discoverability	★★	★★★	★★★★★	★★

Ultimately which tool you decide to go with comes down to what you and the other people in your group are comfortable with. However, our recommendations can be summarised as:

If your group...

- **...organises lots of different things at once** Use Mattermost. The extra features and discoverability should really help to make your group more productive.
- **...organises a lot of actions** Use Mattermost combined with Signal for the added security. Also don't forget to enable disappearing messages.

Choosing a messaging app for your XR group

If you want to create a group chat for your XR group, there are loads of different options and making the right choice can be difficult. In this document we will compare the four apps most commonly used by XR groups: WhatsApp, Telegram, Mattermost, and Signal - which should help you to decide which is best for your group.

We have broken down the comparison into four categories:

- **Security** - How easy is it for the authorities to access your personal information and read your messages? (see the Appendix for more information)
- **Accessibility** - How easy it is for rebels to use the app?
- **Features** - What features does the app have that allow you to organise effectively?
- **Discoverability** - How easy is it for rebels to find and join the group? (see the Appendix for more information)
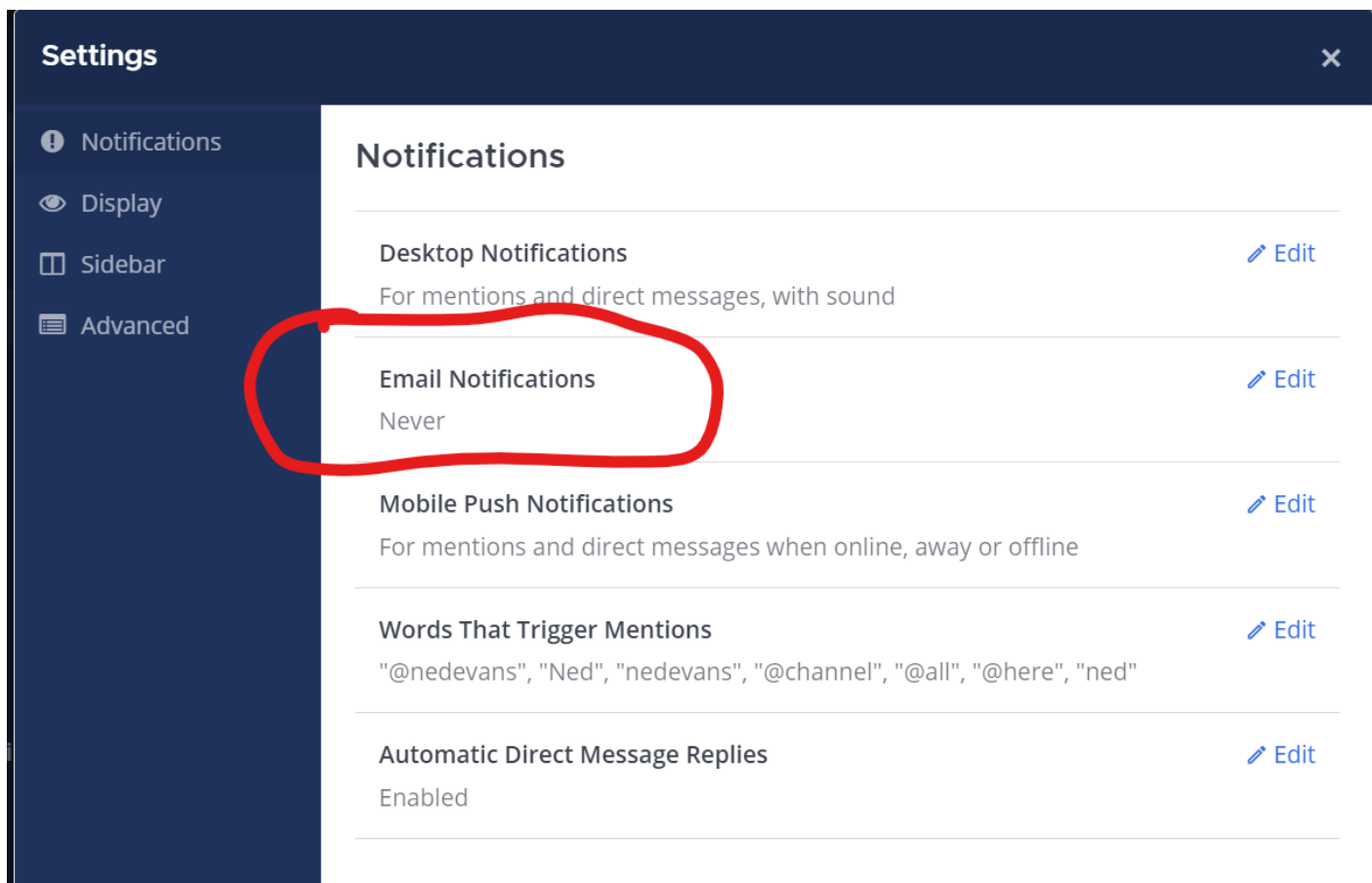
Key Security Information

Mattermost takes quite a different approach to security than the other apps. Instead of employing tactics such as end-to-end encryption and self-deleting messages, Mattermost prevents the authorities from accessing your group's messages by storing them on our own secure server.

The best thing to do to protect ourselves and XR is to use a process called **'Air-gapping'** and is broadly used in government agencies, military and corporate sectors. It's a trick they don't want us activists to know and use!

Air-gapping simply means we communicate any action planning and organising using a **private** Mattermost channel or direct message and then send specific details such as car registrations, credit card numbers and addresses using an app that is end-to-end encrypted and has self-deleting messages (Signal is best). This creates a gap between the planning and those specific details and ensures that if an adversary manages to get their hands on one account, they don't have all the pieces of the puzzle to sabotage an action, nor pair up individuals with a particular action plan, nor put faces to words with intent to commit crime (etc).

PLEASE NOTE: If you are discussing anything 'spicy' / illegal, ensure all members of your private Mattermost channel or group Direct Message, have their email notifications set to **Never**. This adds a level of security as emails potentially can be compromised or 'hacked'. To check your notifications, select the Settings icon - Notifications - Email Notifications - Edit - Never - Save.

Settings   ✕

- ❗ Notifications
- 👁 Display
- ▭ Sidebar
- 🖳 Advanced

Notifications

Desktop Notifications   ✎ Edit
For mentions and direct messages, with sound

Email Notifications   ✎ Edit
Never

Mobile Push Notifications   ✎ Edit
For mentions and direct messages when online, away or offline

Words That Trigger Mentions   ✎ Edit
"@nedevans", "Ned", "nedevans", "@channel", "@all", "@here", "ned"

Automatic Direct Message Replies   ✎ Edit
Enabled

Summary

If you don't want to read the comparison page in full, here is a quick breakdown of the different scores for each messaging app:

	Whats-App	Telegram	Matter-most	Signal
Security	★★	★★	★★★★	★★★★★
Accessibility	★★★	★★★	★★★★★	★★
Features	★★★	★★★	★★★★★	★★★
Discoverability	★★	★★★	★★★★★	★★

Ultimately which tool you decide to go with comes down to what you and the other people in your group are comfortable with. However, our recommendations can be summarised as:

If your group...

- **...organises lots of different things at once** Use Mattermost. The extra features and discoverability should really help to make your group more productive.
- **...organises a lot of actions** Use Mattermost combined with Signal for the added security. Also don't forget to enable disappearing messages.

WhatsApp

WhatsApp is a hugely popular messaging app with over 2 billion users. It's easy to use and the vast majority of rebels will already have it installed on their phones. Does this make it a good fit for your XR group?

Security

Despite being end-to-end encrypted, WhatsApp has a number of serious security issues that make it a poor choice for serious organisation in XR. To start with, it is owned by Facebook, a company whose income depends on collecting people's personal information. You can read WhatsApp's

[privacy policy](#) to get an idea of the sorts of information that they are collecting.

Another serious and often overlooked security issue with WhatsApp is that its end-to-end encryption often does not work. Most WhatsApp users enable an option called 'Chat Backup' so they can recover their messages in case they lose their phone. If this option is enabled, for even a single person in a WhatsApp group, then that means that all of the group's messages will be stored, unencrypted, on either a Google or Apple-owned server, freely accessible to the authorities.

Verdict: ⭐ ⭐

Accessibility

WhatsApp has a lot in common with other messaging apps so it is usually quite straightforward for rebels to learn how to use it. However, in order to sign up to WhatsApp you need a smartphone, which not all rebels will have access to. In order to use WhatsApp on a computer, the smartphone that it's linked to must be connected to the internet continuously, which is a hindrance.

Verdict: ⭐ ⭐ ⭐

Features

You can't save messages for later or mark them as unread so you constantly lose key info and can't find it again. The message box is small and you can't thread effectively so it is difficult to keep track of a conversation.

Verdict: ⭐ ⭐ ⭐

Discoverability

Within WhatsApp, group admins can create and share links that rebels can follow to sign up to the group. This provides a quick and easy way to invite new people. However, unless this link is published somewhere for rebels to find, it is impossible to find the group to join in the conversation.

Verdict:

⭐ ⭐

Other information

Another issue with WhatsApp is that many people use it to speak to friends and family. Having XR-related chats on the same platform can put unnecessary stress on rebels who might want to temporarily 'switch off' XR communications in order to avoid burnout.

Telegram

Telegram is a great messaging app filled with features. In particular it has broadcast channels which can be fantastic for sharing information widely. But is it suitable for group chats?

Security

Although Telegram's website would have you believe otherwise, Telegram actually provides the worst security out of all the apps being compared here (source, source).

One of the reasons why this is the case is because **Telegram group chats are not end-to-end encrypted**. Telegram does allow users to have secret chats with self-destructing messages. However, this is not available for group chats so all of the messages that you send to a group chat will be stored on a server somewhere accessible to the authorities.

Another serious problem with Telegram's security is that **messages are sent using Telegram's own private encryption protocol**, as opposed to something used more widely. This means that it has not been as thoroughly tested and many security vulnerabilities have been exposed in the past.

Verdict: ⭐⭐

Accessibility

Telegram is one of the most accessible apps available. You don't need a smartphone to sign up, just a phone number, and it can be used on practically any device.

Verdict: ⭐⭐⭐⭐

Features

You can't save messages for later or mark them as unread so you constantly lose key info and can't find it again. The message box is small and you can't thread effectively so it is difficult to keep track of a conversation. It's limited in terms of formatting messages and if you want to broadcast and add an image there's a character limit so you have to be able to either fit your message into that limit or miss out key info.

Verdict: ⭐⭐⭐

Discoverability

Telegram has some excellent features that make group chats easy to find and join. Like Signal and WhatsApp, users can share a link to the chat that people can use to join it. However, you can also search for public Telegram channels from inside Telegram. This makes it easy to find and contact broadcast groups but can also lead to spam since anyone can join these channels - even if they are not a member of XR.

Verdict:

Mattermost

Mattermost is the messaging app that has been specially set up by XR for rebels to collaborate with each other. It is quite different to the other apps being discussed because it is designed to be used by teams in a workplace as well as for personal communications. Unlike the other tools, it also

exclusively runs off of renewable energy.

Security

Mattermost takes quite a different approach to security than the other apps. Instead of employing tactics such as end-to-end encryption and self-deleting messages, Mattermost prevents the authorities from accessing your group's messages by storing them on our own secure server.

The best thing to do to protect ourselves and XR is to use a process called **'Air-gapping** and is broadly used in gov agencies, military and corporate sectors. It's a trick they don't want us activists to know and use! Air-gapping simply means we communicate any action planning and organising using a **private** Mattermost channel and then send specific details such as car registrations, credit card numbers and addresses using an app that is end-to-end encrypted and has self-deleting messages (Signal is best). This creates a gap between the planning and those specific details and ensures that if an adversary manages to get their hands on one account, they don't have all the pieces of the puzzle to sabotage an action, nor pair up individuals with a particular action plan, nor put faces to words with intent to commit crime (etc).

Another great advantage to using Mattermost is that if rebels ever get arrested, they can have their accounts temporarily suspended so the police would not be able to read any messages even if they took a rebel's phone. Once the rebel gets out of custody they can then have their account reactivated.

Verdict: ⭐⭐⭐⭐

Accessibility

You do not need a smartphone to sign up - only an email address - and you can easily use it on any device unlike some other apps (e.g. WhatsApp) that only work if linked to your phone.

If you have a computer it is very easy to use since you don't have to install anything - just use your browser. This also means that the messages can be easily read on a larger screen.

Verdict: ⭐⭐⭐⭐⭐

Features

Mattermost has by far the most features out of the apps being compared. It is specifically designed for use by teams, as opposed to personal messaging, and so has a number of advantages over the other messaging apps.

For example, in Mattermost chats are organised into teams, public channels, private channels, and direct messages. This makes it easy to navigate between different chats. Also, Mattermost has a much better way to handle multiple conversations happening in the same channel at once. Whilst the other apps allow you to quote reply to individual messages, Mattermost has threaded conversations so you can see the full history.

You are also able to **save messages** for yourself which makes finding links and key info much easier, **mark messages as unread** to revisit later, **pin** important messages so other people in the chat can find them easily and **store regularly used links such as minutes and eeting links in the Channel Header** for everyone to use removing the need to bookmark/store those links on personal devices.

Writing messages in Mattermost is also more powerful. Not only are you able to edit your messages after you've sent them, but you can use Markdown to format your messages in fancy ways. Great for making eye-catching announcements!

There is a small learning curve when you use Mattermost for the first time because, being designed for teams, it is laid out differently to the other apps. The design is practically identical to other popular messaging apps like Slack and Discord so if you are familiar with those you will have no issues.

Verdict: ★★★★★

Discoverability

One of the main reasons why XR uses Mattermost is to make groups discoverable. Every group that signs up to the XR UK Hub will have public and private group chats created on Mattermost for them as the Hub does the 'heavy-lifting' for you. Having your group on the Hub means the Hub does the work of creating your Mattermost channels (as well as Cloud folder and Forum spaces) and the group's members will be joined automatically to the group's chats and at the same time, given access to the Cloud folder and Forums.

Every group that signs up to the Hub gets a public group chat called a **RECEPTION** channel so, if you're not a member of the group, contacting the group is as simple as searching for and joining the group's Reception. Having public discoverable Receptions is a major advantage over other apps as you can quickly see if a channel already exists for a specific group or topic. After joining a Reception you can then chat to the group and if you want to get more involved, you can be sent a

Hub invite to the group which automatically adds you to the group's private channel. You can't search for chats on WhatsApp and Signal and can only find big public channels on Telegram which leads to similar channels being regularly created for the same purposes on these other apps. This can lead to burn-out for chat Admins as there often isn't the capacity to administer these additional chats and in addition, rebels get added to multiple chats for the same group increasing the number of chats they need to monitor which quickly leads to individual burn-out.

You can also use the Hub Groups List to find other groups and get information such as their email address, website and social media account.

This is why **we strongly recommend that your group at least signs up to Mattermost and the Hub** as it provides an easy way for other groups to get in touch with you.

Verdict:
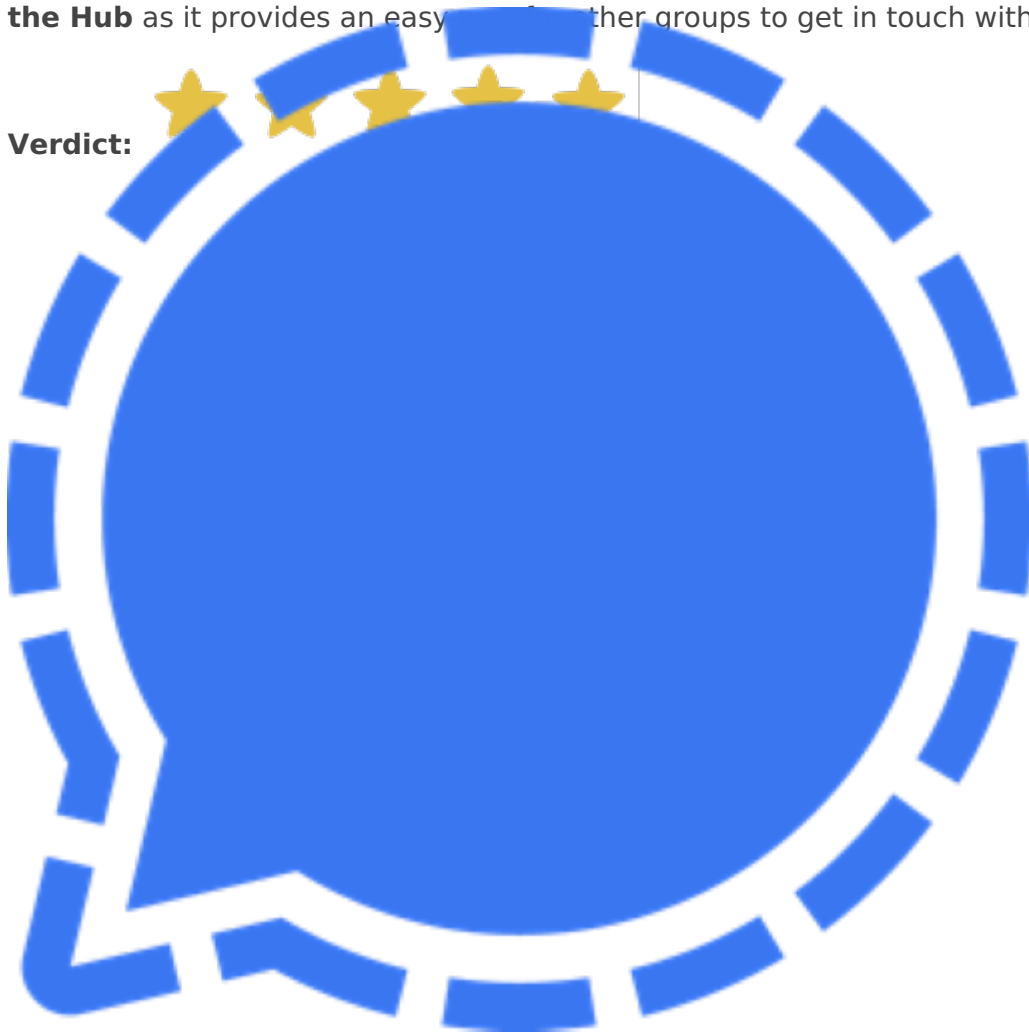
Signal

Security

Signal has unquestionably the best security out of all of the apps compared here. Chats are always end-to-end encrypted and you can enable disappearing messages. Furthermore, Signal is actually open-source. This means that anybody can look at Signal's source code and verify that it is secure.

Verdict: ★ ★ ★ ★ ★

Accessibility

Has complicated features like Signal PIN.

Verdict: ★ ★ ★

Features

Signal has many of the same features as WhatsApp and Telegram. Whilst this makes it easy to learn how to use, it also means that:

- It is hard to write longer messages in the small message box
- It is difficult to keep track of multiple conversations happening at once
- Once you have sent a message it can't be edited

Signal can also be problematic for rebels who have limited storage on their phones because the messages are stored locally instead of in the cloud, and this can take up a lot of space.

Verdict: ★ ★

Discoverability

Just like WhatsApp, you can share links to Signal group chats allowing people to quickly join the group. This is great for signing people up but it is hard for rebels to find this link and join the group.

Verdict: ⭐ ⭐

Appendix

Why does security matter?

Given the types of actions XR does, **it is essential that the authorities do not get access to rebels' personal information and private messages**. This is for a number of reasons including:

- It could compromise the legal defences of arrestees
- It could affect the right of rebels to stay in the UK

When discussing security in the context of messaging apps, there are two main things to think about:

- Can my messages get intercepted?
- Where are the messages getting stored?

The first of these is straightforward - to make sure messages cannot be intercepted we need to make sure that the app uses secure encryption when sending messages. The second, however, is a little more complicated as it depends on terms like "end-to-end encryption".

End-to-end encryption is used by a number of messaging apps. What it means is that the messages are stored on the phones sending and receiving the messages, rather than on some server. This is generally good from a security standpoint because the authorities would need to access one of the phones in order to see the messages; something much harder for them to do than approach the owners of the server with a warrant.

Another important things to consider when choosing a messaging app is whether or not you want

to have disappearing messages. These are messages that are automatically deleted after a certain time period, usually around a week or so. This can provide an additional layer of security on top of end-to-end encryption.

Lastly, one extremely important thing to bear in mind when discussing security is that **by far the biggest weakness in XR's security is the people**. It is very easy for an undercover police officer to pose as a protester and get themselves added to a 'secure' group chat. Once that happens, any security features of the messaging app become irrelevant since the authorities can see everything that is getting discussed.

Why does discoverability matter?

Discoverability - making your group easy to find and get in touch with - is a huge issue for XR. We are a decentralised organisation so each group has the freedom to decide how they want to

organise and communicate. This is fantastic from the point of view of mitigating for power, but it makes it difficult to share knowledge and skills across groups. To try and reduce this problem, it is important when choosing a messaging app to think about how other rebels and groups can find the group and get in touch with you.

Alternative messaging apps

There are many other messaging apps used by rebels in XR. We have just chosen to focus on the most commonly used ones here. Some other popular choices include:

- Discord: An app with some great features but extremely poor security and privacy.

Useful links

- Electronic Frontier Foundation: Thinking About What You Need In A Secure Messenger
- A Guide to Group Chats on Signal, Whatsapp and Telegram book on the Rebel Toolkit

How to set up and run effective group chats

This Chapter is about setting up a group chat on Telegram, Signal and WhatsApp including the benefits and downsides of each communication app.

When setting up the group chat make sure you

When setting up the group chat make sure you:

1. Add a group description so everyone knows why they have been added to the group. This helps to keep the conversation on topic.
2. In the description of the chat include any relevant information including your group agreement and any rules for the chat. If these are too long to be directly added into the description, add a link to a document.
3. Turn off the group link so only admins can add members (There is no group link in WhatsApp)
4. Make at least three trusted people admins including yourself.

Tips and recommendations for moderating a group chat

Hopefully you'll never be in a tricky situation; but sometimes people can troll, spam or act against XR's principles and values on group chats. In general this is less likely to happen on closed, secure chats, but it is a good idea to have 'agreed in advance' rules for this type of behaviour.

1. Always make sure there are at least three admins to moderate the chat.
2. Make sure you have an agreed group agreement in advance. It is up to your group what rules you agree to, but it is best to ensure these rules are agreed to in advance. It also helps for rules to be the same on all platforms you are using to communicate. Ensure that when people sign up to the group they are pointed to the group agreement so they know what they are agreeing to, or that they are shown it before joining the group.
3. Follow a 'two strikes and you're out' policy. On the first occasion of 'misbehaviour' an admin should remove the person/people from the group, private message them to explain they have been removed, and calmly explain why (citing the rules you have agreed). On the group chat itself that they have been removed from, explain that you have removed them from the group and why. If you have a group agreement in place most people will know the policy and know what will happen if there is bad behaviour on a group chat.
4. Give the removed person a cooling-off period and discuss re-adding them to the group provided they are willing to follow the group agreement. Ideally, if the person is happy to apologise, and wants to be added back into the group then you can add them back in, on the basis that there is only one more chance. As we said, if this is covered in the group agreement policy in advance, and everyone knows what happens in a bad behaviour situation, then nobody should be upset about this. Once that person has been let back into the group, admins should ensure that ongoing conversations are monitored and enforce the 'two strikes and you are out policy'. If necessary, you may need to remove them from the group conversations permanently, and you may also want to assess whether or not you want them involved in the XR Local Group, Community Group, or Working Group at all.
5. You may decide in your group on a zero-tolerance policy for some misbehaviour. For example: spamming (so spammers are removed straight away) and also inappropriate sexual behaviour, stalking behaviours, violent threats etc.
6. With the other moderators (ideally 3 or more) take it in turns to do the moderation, and make sure there is some kind of system where you know who is covering what and if somebody is going to be away (So you are not all away and off chat at the same time!) Make sure you provide each other with support because it can be quite stressful if it all kicks off on a chat. Just make sure that moderators also follow the policy, and are ready to

be challenged and justify the removals from a group - so make sure you choose people that understand the rules that the group have agreed, and are tactful and not using it as a power trip!

7. If something comes up that is part of a long running dispute that you do not feel able to deal with within the group, we recommend that you contact the XR Transformative Conflicts team by emailing xr-conflict@protonmail.com

We know that this task seems a bit onerous at first and everyone is generally quite happy on XR chats, but we really can't stress enough how important it is to make sure difficult or contentious situations don't escalate and also that everybody knows what the rules of behaviour are on the chats.

Keeping Group Chats secure

This chapter is about keeping Group Chats secure. It will describe the benefits and downsides in terms of security of the different communication apps Signal, Telegram and WhatsApp as well as give guidance as to how to keep a Group Chat secure.

Comparing Security of Signal, Telegram and WhatsApp

Signal

• Signal is by far the most secure encrypted channel option.

• When you use Signal, your data is stored in encrypted form on your devices.

• Signal also has disappearing messages (self-destructing messages) which the other channels do not, which are an essential security feature

• Signal is free and all you need is a smartphone.

• Unlike Telegram, which also benefits from end-to-end encryption in its "secret chats", Signal has the feature enabled by default so you won't have to take any additional steps to get this, and that is why it is used for actions over and above everything else.

Telegram

• End-to-end encryption is not automatically used on messages sent in Telegram.

• Telegram is really a social media platform and has a very 'relaxed' content moderation strategy- this means it is targeted by spammers. You have to be on top of moderating it!

• Telegram is very useful for broadcast channels (in which only admins can post). Links for these can then be shared on wider channels (eg. Rebellion Broadcast). However, widely shared links attract spammers so they need to be carefully moderated.

WhatsApp

• End-to-end encrypted but owned by Facebook therefore its privacy is not reliable. WhatsApp also collects more metadata on you than apps like Signal.

• We do not recommend that anyone uses WhatsApp for actions, even those that are 'non-spicy' just in case.

• Some groups choose to use WhatsApp as more people already have it downloaded, but due to the security issues described above we strongly recommend groups use Signal for all of their organising.

See Also

Choosing a messaging app for your XR group in the "Online Tools for Communicating with Other Rebels" book.

Guidelines to keep the Group Chats as secure as possible

When setting up the group chat make sure you follow these rules to keep it as secure as possible

1. Make sure that you add a group description, so everyone knows why they have been added to the group.
2. In the description of the chat include a URL link to any relevant information including your group agreement and any rules for the chat.
3. In settings turn off the group link (There is no group link in WhatsApp)
4. Make sure that only admins can add members or access the invite link.
5. Make at least three trusted people admins including yourself.
6. If actions are happening soon, make sure you set disappearing messages to a day or a week otherwise 4 weeks should be fine (WhatsApp and Telegram do not have this ability)

Security on chats

1. Ideally only add people that you know well or are verified by others (trusted rebels)
2. If you are doing spicy actions make sure people use pseudonyms and burner phones if possible, and that those are added to the correct chats (Normal names and numbers removed).
3. Make sure there are separate secure chats for action days or spicy actions so that you can delete them afterwards.
4. Make sure only admins can add new members to the chat.
5. Make sure you set disappearing messages.
6. Make sure you keep the group links off.
7. Remember that many chat platforms attach media and files and links separately, so admins should regularly check that old media files and links are deleted
8. After the chat is done, and everyone has agreed that the group chat is done with, leave the group and delete the chat off your phone
9. Some members may not do this, so once the chat is done with, admins can remove members individually and then delete the chat off phones by deleting the group chat altogether - in this way people are not on lots of different chats that have ended which may cause security issues should someone's phone be seized.

# Hide your phone number from others using Telegram

By default, when someone joins a Telegram channel their phone number is visible to all others in the channel. This can lead to the person being contacted by, for instance, spammers. Some have been contacted in WhatsApp using the number gleaned from Telegram. The Direct Message facility in Telegram can be used to contact someone without involving their phone number.

The settings in Telegram can be changed to remove the visibility of the phone number.

To make the number not-visible in all your Telegram channels. The steps are almost exactly the same on a phone as a desktop or laptop.
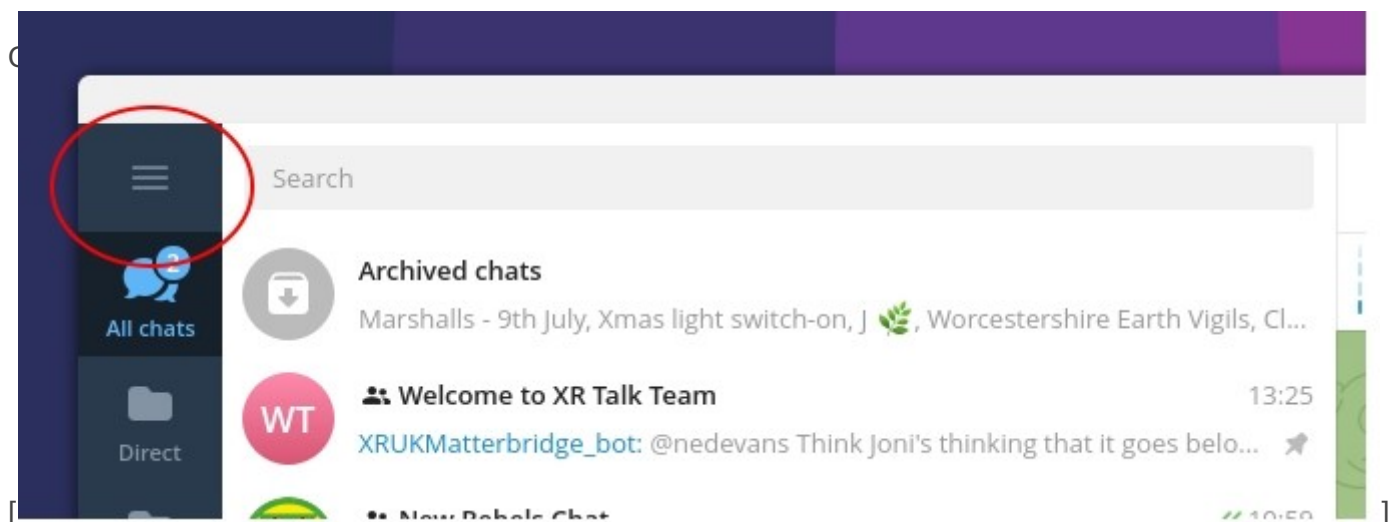
Click **Settings**
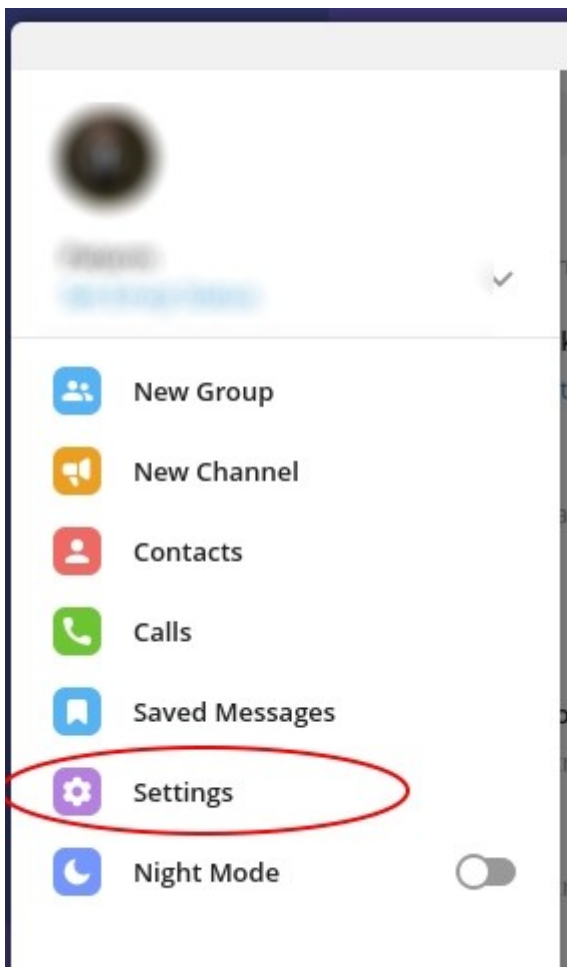
Click **Privacy and Security**
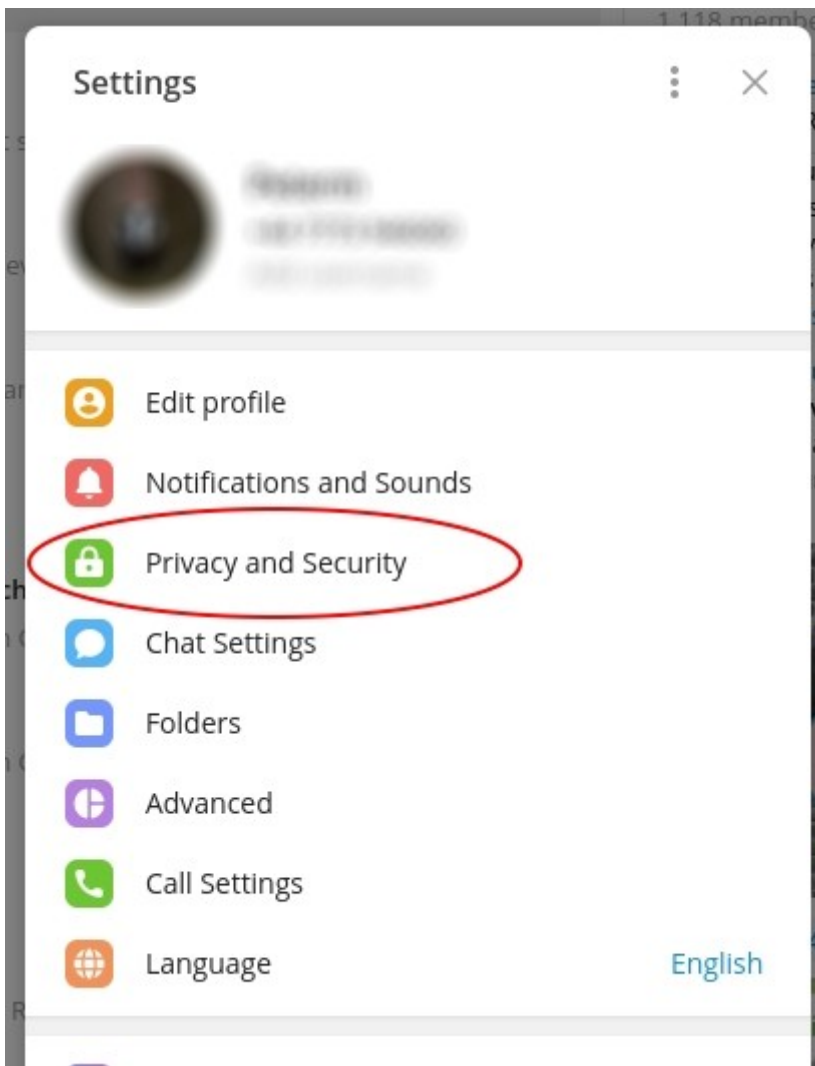
In the Privacy section click the text to the right of **Phone number**, change the setting to `Nobody` or `My contacts` depending on who you trust.

You will then see an overview of your setting, and note that there are a few other settings that could also be changed.

Then **Save**

There doesn't appear to be a way to make the 'hide number' the default for everyone joining the channel.

Telegram: How to remove spammers

Spamming can be an issue with Telegram chats.

If you receive direct messages [DM] from random people on Telegram saying things such as, 'Hello' or 'Hello, what are the XR groups doing?' or similar - simply report, block and delete immediately. If you engage with a random DM then you'll find yourself in a conversation, the spammer will try to engage you for as long as possible resulting in either asking for money, help with transferring funds or something along those lines.

How do spammers get into groups?

If the invite link to a Telegram group chat is public, then anyone can join!

If members can share the group's invite link, it can end up anywhere.

To:

1. remove someone from a group chat
2. delete all of their messages
3. report them to Telegram (although it's not known if this has an impact).

First, **you need to be an Admin of the chat group.** Please share the workload by making other trusted rebels Admin, after getting their permission to be made an Admin.

You can complete this process either on a phone or by using your laptop/desktop computer to access Telegram.

Please be aware that some spammers will join the group and quickly change their name to stop you finding and removing them, so try to complete this process quickly.
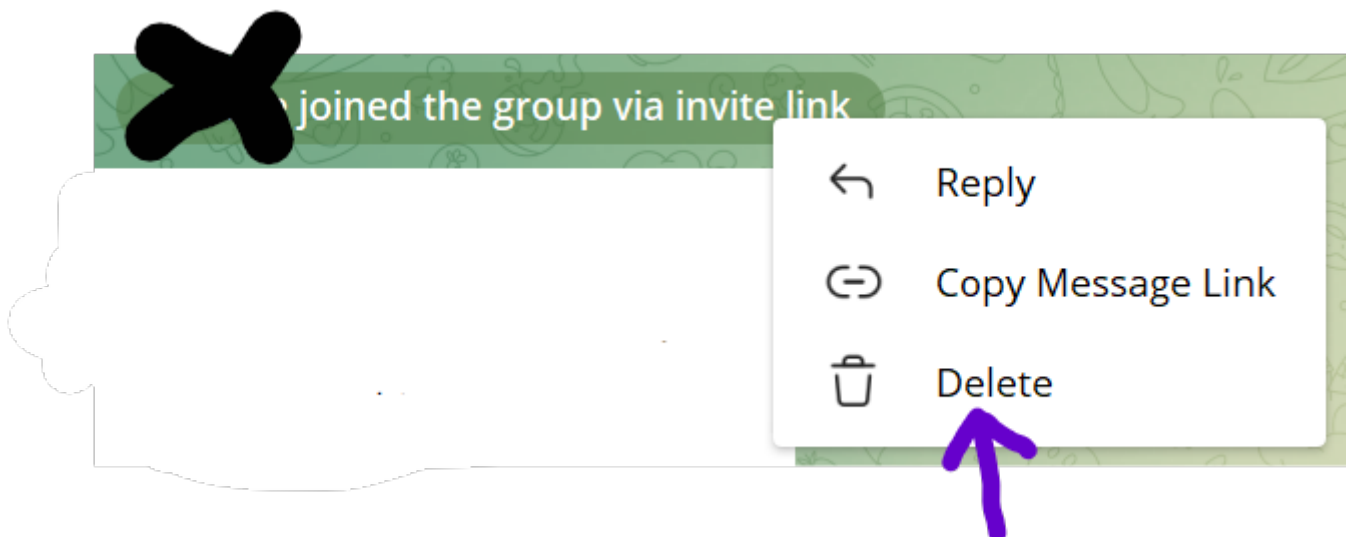
- Find where the spammer joined the chat via invite link.
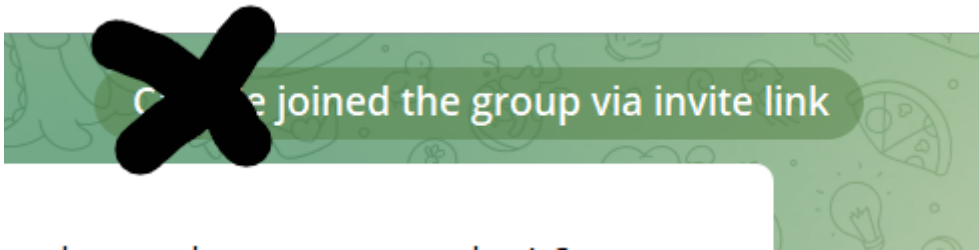
- **On a phone** - tap to the right of their name on the words 'X joined the group **via invite link'.**
- **On a computer** - right click on the words 'X joined the group **via invite link'.**
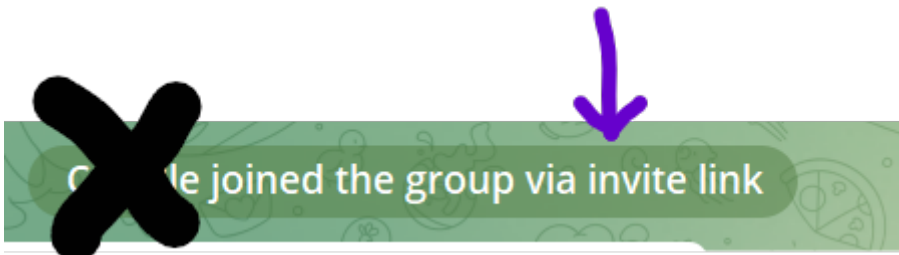
- Select Delete.

- Select the 3 tickboxes: Ban user, Report spam and Delete all from X.

Do you want to delete this message?

☐ Ban User

☐ Report Spam

☐ Delete all from ▇▇▇▇▇▇

Cancel   Delete
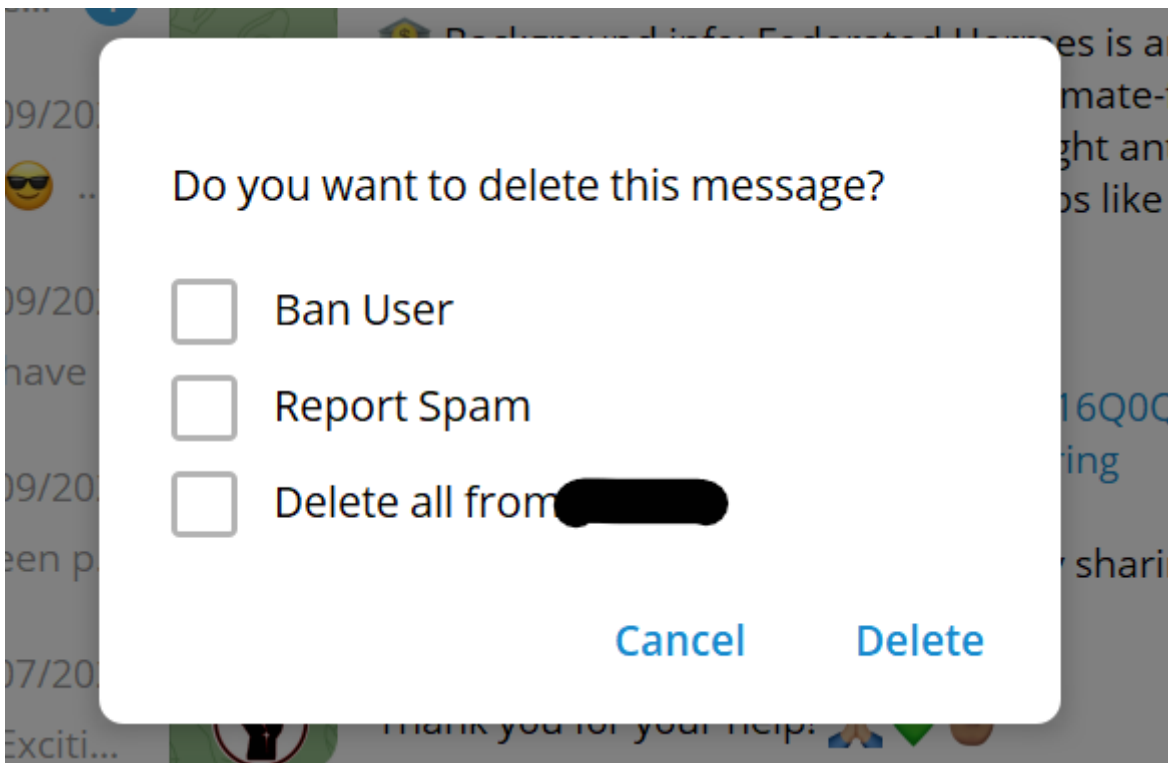
If you simply search for a spammer from the member's list and block and report them from there, that only blocks / reports the spammer for yourself rather than the whole group and it also doesn't delete any spam messages they may have posted.

If you want to 'revoke' the current invite link so spammers can't use it to join or share with other spammers, and create a new invite link to be shared with only trusted rebels - again you'll need to be an Admin.
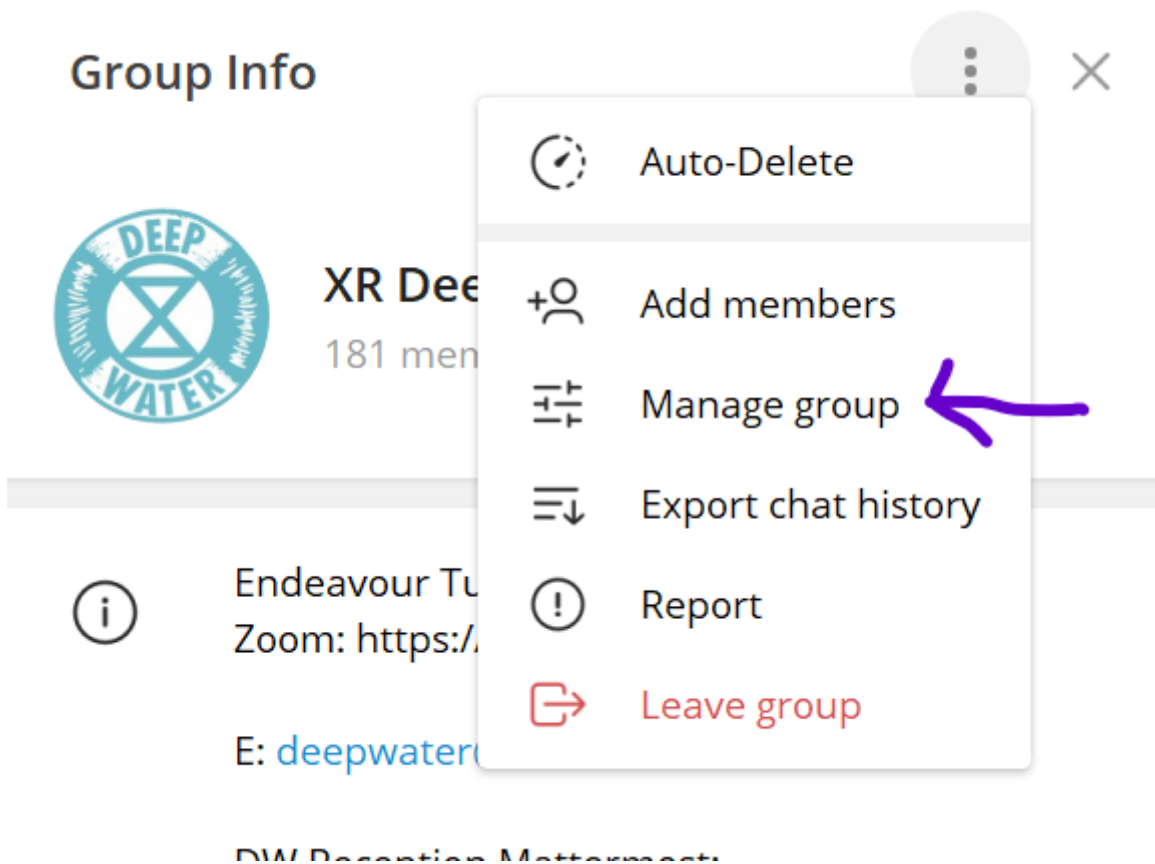
On a phone:

- tap the name of the group and then select the pencil icon
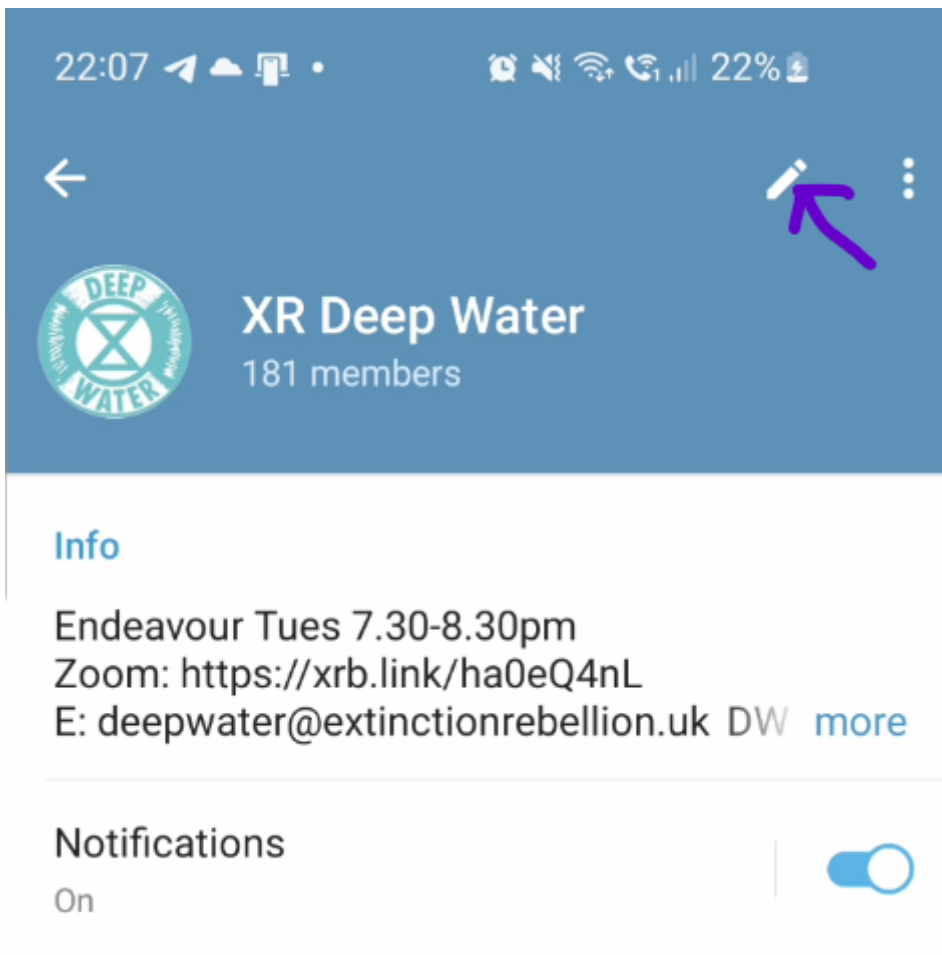
On a computer:

- select the 3 dots and then Manage Group

- select Invite Links
- select the 3 dots to the right of the current Invite Link (it will be called Primary Link on a computer) and choose Revoke Link
- Create a New Link then share that with trusted rebels

To change Permissions so spammers can't add more spammers/bad agents to your group

- select Permissions and switch off 'Add Users'

Changing Your Personal Settings

Prevent Random People From Adding You to Telegram (Spam) Groups

- Select Settings - this will be under the 3 horizontal lines
- Privacy and Security
- Groups & Channels
- Who can add me to group chats? Select My Contacts

Although this will mean that only those in your Contacts can add you to Telegram chat groups, you can help speed up the process of getting into chats by adding all trusted rebels to your Contacts.

If your phone number is visible to all, spammers can find this and then add you to spam groups or direct message (DM) you using your number.

To hide your number:

- Settings
- Privacy and Security
- Phone Number
- Select either My Contacts or Nobody
- If you select Nobody, you also have the additional option of 'Who can find me by my number' i.e. if a trusted rebel has your number but it isn't in their Contacts, they can search for you on Telegram by using your number.
- Select either Everybody or My Contacts

If you're interested in Telegram bots, there are ways to stop spammers using these.

Telegram and Mattermost

Please bear in mind that XR has Mattermost where we can use channels for chats, a Team's Town Square and Off-Topic for announcements to all Team members and we can build one or two-way bridges between Mattermost channels and Telegram groups/channels.

Using the Hub and Mattermost is more secure than Telegram because:

- Only Group Admins can send out Hub invites to members
- Once the member has accepted their Hub invite they then are added the group's Team and/or Channels on Mattermost
- Group Admins will only send out invites to those they've 'met' either via Zoom or in-person, or because another trusted rebel has passed on the new member's email or handle for an invite.

If you'd like to know more about the Hub, please select this link

A bit of fun!

And while we're on the subject - one of the things that's brought me a moment of joy recently... I've found that when I get joined to a spam group, instead of immediately reporting and leaving the group, I spend one minute sending hundreds of XR stickers and gifs into the group. And invariably **I get removed for spamming!**

If you want to find the XR sticker pack and gifs.

- tap the emoji icon
- select the sticker or gif icon
- use the magnifying glass to search for extinction rebellion (try XR if using the long name doesn't work for you).
- select the stickers and gifs and send the spam group some XR love!

Chat Etiquette for XR Group Chats

Here are a few Chat Etiquette Guidelines that are being used in XR Group Chats whether on Signal, Telegram or WhatsApp:

• Welcome newcomers!

• Please follow XR's principles & values

• Avoid swearing

• Ideally keep discussion between 7am and 11pm

• Answer questions and make sure people feel heard

• Post off-topic messages in a more suitable channel

• If people leave the chat in response to a post, this is a sign of overheating - slow down, pause and reflect

• Take two-way conversations out of the chat. Don't send unsolicited messages. Harassment will not be tolerated.

• Send a longer message over lots of separate ones; people then have the chance to opt in to read more.

• Avoid encouraging anyone to vote or not vote for a political party.

• Don't attribute info from this chat elsewhere, like quoting from it publicly and naming the originator.

• Avoid posting sensitive action info which can later be used as evidence

Online Behaviour Guide

XR's Regenerative Culture

We owe each other a duty of care to make our presence on our communications platforms a comfortable and beneficial experience. This includes a healthy focus on mutually supporting through:

- Self care – how we take care of our own needs
- Mutual care – how we take care of each other
- Interpersonal care – how we take care of the relationships we have, being mindful of how we affect each other
- Community care – how we take care of our development as a community

Etiquette and Standards for Posts

When posting messages we recommend that contributors:

- Be respectful – people are different; we all have strengths and weaknesses and different backgrounds – consider your audience
- Use 'I' statements
- Practice compassion by putting themselves in others' shoes
- Take the time to read, re-read, and reconsider before posting

When using the chat channels and forums, we ask all contributors to have care for the community, offering a harassment-free space for all to participate, embracing our unique differences. We then cultivate this respect for each other, both within project spaces and in the wider public arena where we represent the XR community.

Positive Behaviours

- Use welcoming and inclusive language
- Be respectful of differing viewpoints and experiences
- Be willing to engage with feedback (constructive criticism)
- Focus on what might most be in service of the community as a whole
- Cultivate curiosity and an empathic awareness towards other community members

Negative Behaviours

- Avoid sexism, racism, classism, and any other prejudices
- Be aware that we all have things to learn and we all make mistakes
- Avoid making assumptions and be open to listening and learning if challenged

- Do not employ harassment, either public or private, including trolling insulting/derogatory comments, bullying, personal or political attacks
- Do not publish others' private information without explicit permission
- Avoid conduct which could reasonably be considered inappropriate in a professional setting

Maintaining good behaviour falls to all of us

If we find a post that strays from the above guidelines, it's up to each of us to feed back our concerns, initially to the originator of the post and, if necessary, to a Moderator/Group Admin, by Direct Message. Either way, we should be sensitive with any language, but, as our regenerative statement says: "[we have] cultures of respect and listening, in which people deal with conflicts when they arise, feeding back quickly and talking about disagreements and issues without blaming and shaming." If you find a post that you believe needs moderation, reply directly to it and explain why and, if appropriate, suggest to the poster a potentially more acceptable way of making their point.

How to find information in a group chat

You're pretty sure you've heard about a protest going on in Derby soon, but don't remember the details, or in which specific chat you've seen the information?

Both Telegram and Signal allow us to search for keywords, in a specific chat and even in all your chats at once!

Check this tutorial out to learn how to make good use of the search function.