Internal Comms

To be successful, you need great lines of communication with your group and supporters.

- Online Behaviour Guide
- Communicating with Your Group
- Email Accounts and Email Lists
- Messaging Apps: Choosing an App
    - Messaging Apps Overview
    - Security and Discoverability
    - WhatsApp
    - Telegram
    - Mattermost
    - Signal
- Messaging Apps: Administrating & Moderating Chats
    - Keeping group chats as secure as possible
    - Moderating a group chat
    - Template Group Agreement
    - Telegram: How to remove spammers
- Messaging Apps: Broadcast Channels
- Documents
- Style Guide

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 mutual support 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 contributors should:

- 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 chat channels and forums, all contributors have a duty of care for the community, offering a harassment-free space for all to participate, embracing our unique differences.

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 of service to 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- Do not publish others' private information without explicit permission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 messages or comments stray from the above guidelines, it's up to each of us to feed back our concerns in a sensitive way depending on the platform being used. 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, see the moderation chapter for guidance.

Communicating with Your Group

To be successful, you need great lines of communication with your group and supporters.

You should also have a set of comms channels appropriate for different audiences. This will vary from group to group, but the following is typical:

- An email account, so you can communicate with people and other orgs by email without using your personal account
- An email list, for one-way comms with your group and supporters.
- A messaging app for two-way comms with other organisers, e.g. Mattermost or Signal
- A messaging app for one-way ("broadcast") comms with your group and supporters (useful for larger groups)
- You might use the "events" feature of Facebook to communicate upcoming actions, trainings, and meetings
- Documents, for sharing detailed information

Your comms will be busiest when you're organising an action. There's more detailed guidance in this page of the Action Planning book.

In addition to the above comms channels, if you have "sub groups" (maybe you're organising a nation/region or community group) then you should have a network of reps from each group in a shared chat and, when appropriate, a regular meeting.

Email Accounts and Email Lists

There are two types of email to think about...

Email Accounts

An email account for people to have two-way conversations with you. This is the equivalent of your personal email account, but for your group instead. You could use a large email provider (eg. Gmail, Protonmail) or you could apply for one from XRUK e.g. groupname@extinctionrebellion.uk.

The benefits of applying for one ending in extinctionrebellion.uk are:

- if you ever lose access to it you can ask for a password reset
- you can easily share access to it between a few people

Apply for an @extinctionrebellion.uk email account here.

Email Lists

An email list is where supporters can sign up and receive updates from you. This is a way to email large groups of people all at once. You can still put a 'reply-to' address, so that individuals can reply with a questions. Your emails should be 'on message' and jargon-free, because people on your list might be interested members of the public who are not yet involved - and maybe even a few journalists too!

Good ideas for emails are: single-topic emails telling people about an event or action that is coming up, or newsletter style roundups of everything that's happened recently.

XR uses a system called 'Action Network' to store your list of email subscribers and send mass emails to them. It is funded centrally, GDPR compliant and available to all local groups. You can read more in the Action Network overview.

The benefits of being part of XRUK's Action Network system are numerous and you can read more here about why to use Action Network as opposed to other systems such as Mailchimp. Being part of this network helps you pick up more subscribers because you lists will be automatically

promoted for you in a number of ways - read more here

For information and support:

- Read the Action Network for XR book
- Sign up to training with this form
- Message the Action Network Reception on Mattermost or email them at datateam@extinctionrebellion.uk

Messaging Apps: Choosing an App

An overview of messaging apps and detail on the four main ones: WhatsApp, Telegram, Mattermost and Signal

Messaging Apps Overview

As a decentralised network, there is no one communication tool that everybody uses. That can sometimes make it tricky to connect with people. Don't worry, you're not alone!

To help you create a group chat, we will compare four apps most commonly used by XR groups.

Ultimately the app you choose comes down to what you and the other people are comfortable with, including how safe and secure you need to be. If security and organisation are your priority, you may well choose more than one app and use them in combination.

To help minimise information overwhelm, try to plan what chats you need carefully and use existing chats where possible, rather than creating more new ones.

> Communication channels for a specific actions work a bit differently. If you need secrecy and safety, create temporary channels with just those who need to know (with disappearing messages) and use "airgapping" to break up the information flow where appropriate. Delete these channels after use. Head over to this page for lots more detail on how to do secure internal comms for an action.

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.

Overview

WhatsApp

WhatsApp is widely used by people outside of XR but it is not secure so is not great for organising. It doesn’t sync up with Mattermost.

However, Whatsapp Communities can be very useful for keeping all of your (non-spicy) comms in one place. A community is a collection of chat channels, and individuals can choose which ones to join. Each community also has a central Broadcast-only channel.

More detail on WhatsApp here.

Telegram

Telegram is used for XRUK's broadcast channels.

It’s an encrypted messaging service with lots of features. You can edit and pin messages, see the chat history after you join a channel, locate media, and each chat can hold a large number of people. It’s also accessible on nearly any device. A limit on message word count can impact broadcast posts.

Telegram has some good features that Whatsapp does not have.

However, there have been recent concerns about the security of Telegram, as not all messages are End to End Encrypted and there is a lack of transparency around who Telegram is sharing its data with.

More detail on Telegram here.

Mattermost

We run our own dedicated communication tool, called Mattermost (if you're familiar with Slack or Microsoft Teams, it's a bit like those). We host it on our own secure servers powered by renewable energy and it is accessible on both phone or computer.

It is used by most XRUK teams and is also available to all groups. It's a great way to connect to any group or team in the movement: look for the dozens of "reception" channels, where you can pop in to ask questions. You can also connect directly with individual users by direct message.

However, users who are not used to this sort of platform can sometimes find it overwhelming or confusing, which is why many local groups choose other platforms.

There is lots of help and support here on Rebel Toolkit.

More detail on Mattermost here.

Signal

Signal is widely used by action planning groups and organisers. It’s the most secure encrypted chat with a disappearing message function. It’s also visually clean and crisp.

However, it’s not possible to pin or thread messages or edit your messages after 15 minutes, making it less useful for mass communications.

More detail on Signal here

Summary Table

	WhatsApp	Telegram	Mattermost	Signal
Security	★★	★★	★★★★	★★★★★
Accessibility	★★★	★★★	★★★★	★★
Features	★★★	★★★	★★★★★	★★★
Discoverability	★★	★★★	★★★★★	★★

Security and Discoverability

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.

If you're organising actions, head over to the Internal comms for your action page to read about chat security in more detail.

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 self organising, 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 your group and get in touch with you.

WhatsApp

WhatsApp is a hugely popular messaging app with over 2 billion uers. 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. They can't read your actual messages, but there's still lots of metadata they can collect. You can read WhatsApp's privacy policy to get an idea of the sorts of information that they are collecting.

Another issue with WhatsApp is that it makes it easy to backup chats to a cloud storage like iCloud or Google Drive, and that the option to make these backups encrypted is off by default. That means that any user in your chat who has a backup running (which is common) and hasn't manually set this to be encrypted will be uploading the whole chat (their messages and everybody else's messages in the shared chat) to a server. The data on that server can be read by the company or by security services with a warrant. However, you can now add End to End Encryption to this backup.

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.

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. However, you can pin key chats so that they remain at the top of the chat list. The message box is small and you can't thread effectively so it is difficult to keep track of a conversation.

Whatsapp have recently launched a new feature called Communities, which allows you to collect together multiple chats for your group into one space. Each community has a broadcast only channel that everyone in the community is subscribed to, and then you can add as many sub-groups as you like. This means chats can be arranged by topic, making it easier to keep on top of conversations. Each member can choose which chats they want to join, reducing information overwhelm from being in too many chats.

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.

The Whatsapp communities feature improves discoverability of channels once a person is in that community, as all chats connected to one group can be connected together.

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 [1] [2].

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.

It can be compromised if malware is installed on the phone or computer, or other people have access to that device if they use your login. Or if you have infiltrators - no app protects against those.

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.

Features

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

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.

Use this information to help you hide your details from spammers.

And this information about removing spamers.

Drawbacks

Telegram is really a social media platform and has a very ‘relaxed’ content moderation strategy- this means it is targeted by spammers if you have open channels. You have to be on top of moderating it!

Some people find it difficult as you can't save messages for later or mark them as unread so you constantly lose key info and can't find it again. However, you can pin key threads at the top of the chat list.

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.

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

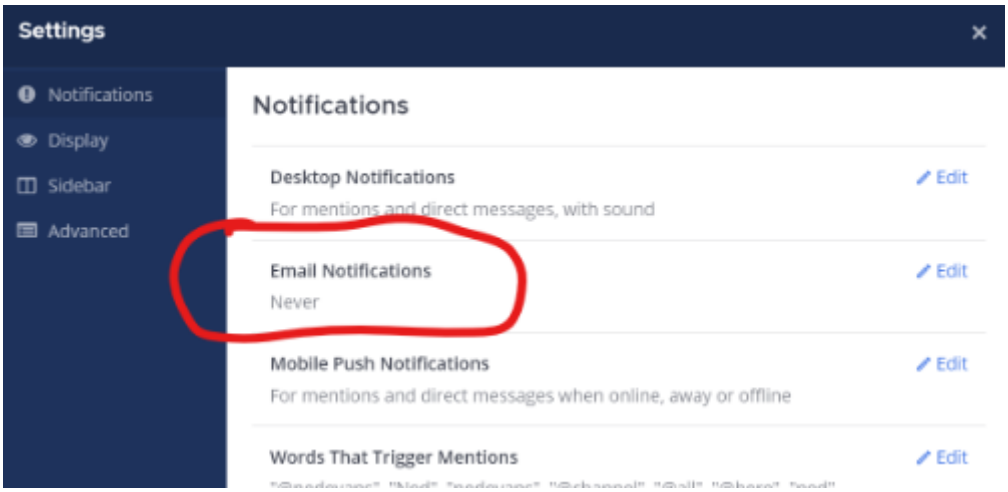
Mattermost takes quite a different approach to security than the other apps. Instead of employing tactics such as end-to-end encryption and self-deleting messages, Mattermost prevents the authorities from accessing your group's messages by storing them on our own secure server.

Its great to use Mattermost as one of your channels if you are **air-gapping** to separate out information on a need to know basis.

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.

Can be compromised if malware is installed on the phone or computer, or other people have access to that device if they use your login. Or if you have infiltrators - no app protects against those.

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.



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.

However, some rebels who are less 'techy' find the different format of Mattermost (as opposed to a messaging app like Whatsapp or Signal) very confusing, which is why Mattermost isn't used by some Local Groups.

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 meeting 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.

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 publicly 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 well as rebels when they need to monitor multiple chats for the same group/action.

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.

Signal

Security

Signal has 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.

Signal has been designed with security in mind, not bolted on afterwards, so the defaults are more likely to be good.

Signal PIN is a useful application lock, although this isn't set up on the computer version.

Signal encrypts local information on your computer or phone so that it's only visible through the app or computer programme.

It can be compromised if malware is installed on the phone or computer, or other people have access to that device if they use your login. Or if you have infiltrators - no app protects against those.

Accessibility

People aren’t normally familiar with Signal before joining XR so may be a barrier to newcomers or less technical users.

Has complicated features like Signal PIN which can be a barrier to use.

It is available on computers, although it'll still be tied to your phone number.

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
- Can be used on smartphone and computer versions

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.

Drawbacks

It can be hard to know who is on a Signal chat, as names can be changed and phone numbers hidden. Like with all chat apps, be careful who you are talking to if that's important.

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.

The "metadata" about who's using the app and where they appear to be may be available to the authorities if they can track the connections to the central computer server, or get access to that

server.

Messaging Apps: Administrating & Moderating Chats

Keeping group chats as secure as possible

Larger chats such as Local Group chats cannot practically be kept completely secure, because you need to be able to welcome new people into them. It is therefore important to make it clear that these chats are not secure, and no 'spicy' information should ever be shared in them. You may want to allow people to add their friends etc to the chat, so it might not always be appropriate to follow all of the advice below. Use your judgement to follow relevant recommendations.

Standard security measures

1. Don't publish invite links to chats on websites or social media unless they are for 'broadcast' type channels on Telegram or Whatsapp.
2. Always have multiple 'admins' for a chat group, to help to remove posts or spammers.
3. Read the page on moderating a chat.

Higher security suggestions

1. Ideally only add people that you know well or are verified by others (trusted rebels).
2. Make sure only admins can add new members to the chat.
3. For Signal remember if you add someone by mistake and remove them, they can still see the info in the header of the chat.
4. 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 with their normal names and numbers removed.
5. Make sure there are separate secure chats for action days or spicy actions so that you can delete them afterwards.
6. Make sure you set up disappearing messages. If actions are happening soon, make sure you set disappearing messages to a day or a week. Otherwise 4 weeks should be fine. Only Signal can do this automatically, however Admins in Mattermost, WhatsApp and Telegram can delete others' messages.
7. Make sure you keep the group 'invite links' off.
8. 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.
9. 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.
10. 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.

11. Use the XR Cloud or CryptPad instead of Google Docs. See Document Management.
12. If you are using chats for actions read more about 'air-gapping' here.

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. It is important to make sure difficult or contentious situations don't escalate.

1. Always make sure there are at least three trusted admins to moderate the chat. Create a separate, private chat for these moderators, so there's a space for people to support each other in response to questions or queries. Take turns to do the moderation.

2. Name the chat and use the header/description to make it clear what the chat is and why people have been added. Make sure that only admins can add members or access the invite link by turning off the group link in settings (there is no group link in WhatsApp). Be aware of where the invite links are posted, e.g. don't add private invite links to websites or social media as spammers will find these and join your group chats.

3. Create a group agreement. 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 that 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. Link the group agreement from the chat header/description.

4. Welcome newcomers. Answer questions and make sure people feel heard. Regularly remind everybody of chat etiquette. Chatting informally to build momentum in the public chat is best done from personal accounts, rather than anonymous admins.

5. Block and report spammers. See here for how to manage spammers in Telegram.

6. Avoid posting sensitive action info, naming organisers or any info which can later be used as evidence. Also be aware that infiltration is common on open chats, so don't share anything that can be used against people as evidence.

7. If a member of the group keeps posting off-topic messages or dominating the space then respectfully ask them to stay on track, or switch to a more suitable channel. Create another space for them to be heard. If they continue, follow up with a direct message, or ultimately consider blocking them from the chat with an explanation. Make sure that moderators follow the policy and are ready to be challenged and justify removals.

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

9. 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 to). 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. You may decide in your group on a zero-tolerance policy for some misbehaviour.

10. 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.

Here are the Mattermost Moderation Guidelines used on public XRUK channels.

Template Group Agreement

‘Chat burn out’ is a very real thing, something well studied, and ensuring discussion is kept out of chat, and chat is kept out of discussion takes work.

This is important work, as it keeps our communication and knowledge synthesis environments healthy, enjoyable and productive.

The basics

- Adhere to XR's Principles & Values
- No spamming
- No racism, sexism, hate speech
- No pornography or violent imagery
- Don’t randomly add people to the channel without consent
- Don't post the first names or contact details of anyone without their consent
- Be excellent to each other!

Moderation Policies

Two Strikes policy

Posts that are harmful/destructive in nature (for instance, advocating violence) and posts that breach the Principles & Values will fall under a Two Strikes policy. This involves a warning and explanation, with a further overstep resulting in the person being removed from the chat.

Examples:

- Racist, sexist or posts of a harassing nature
- Ad hominem attacks- posts that breach the Principles & Values (for instance advocating violence)

Three Strikes policy

Posts that are considered spam, trolling, or aim to co-opt support, will fall under a Three Strikes policy. This includes posts that use the @all or @channel or @here notifications, as is posting the same message across many channels (cross posting). Adding rebels to groups or channels without

their permission is also considered spamming.

Posters that advertise personal projects or call for rebels to join movements outside of XR also apply. As will apparent trolls.

Examples:

- Posts calling for XR rebels to join other movements
- Posts espousing denial of climate and environmental sciences
- Posts to multiple channels that do not fit the purpose of the chat

Off topic Policy

Off topic posts are reasonably inevitable. However should chatter start around such an off topic post, it can quickly add noise to a channel, and so stress our communication streams. Authors of such posts need to be gently encouraged to take their topic to a more appropriate channel.

Telegram: How to remove spammers

Spamming can be an issue with Telegram chats.

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!

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.

If you have a spammer in your chat you will want to:

1. Remove them from the group chat
2. Delete all of their messages
3. Report them to Telegram (although it's not known if this has an impact)

Some spammers will join the group and quickly change their name to stop you from finding and removing them, so try to complete this process quickly. You can follow the steps below either on a phone or on your laptop/desktop:

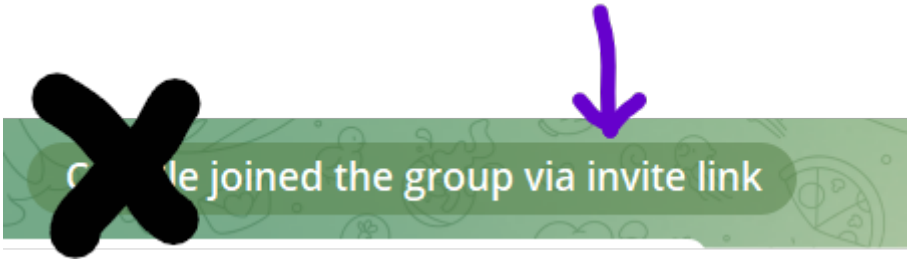
1. You need to be an admin

Please share the workload by making other trusted rebels admins.

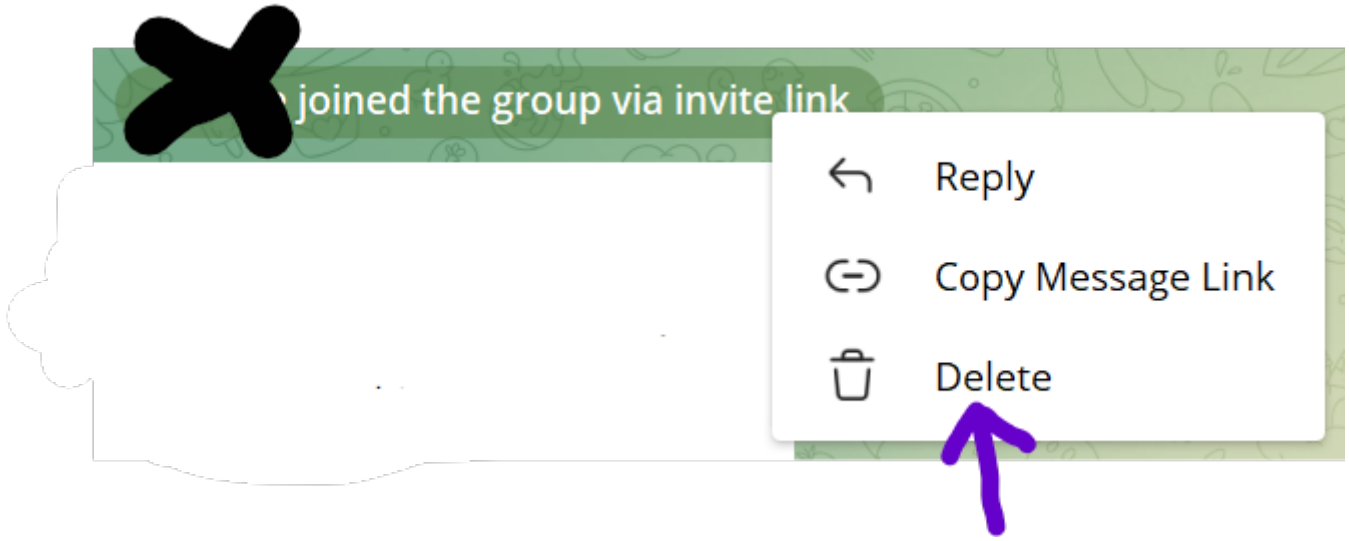
2. Find where the spammer joined the chat via the invite link

3. Right click

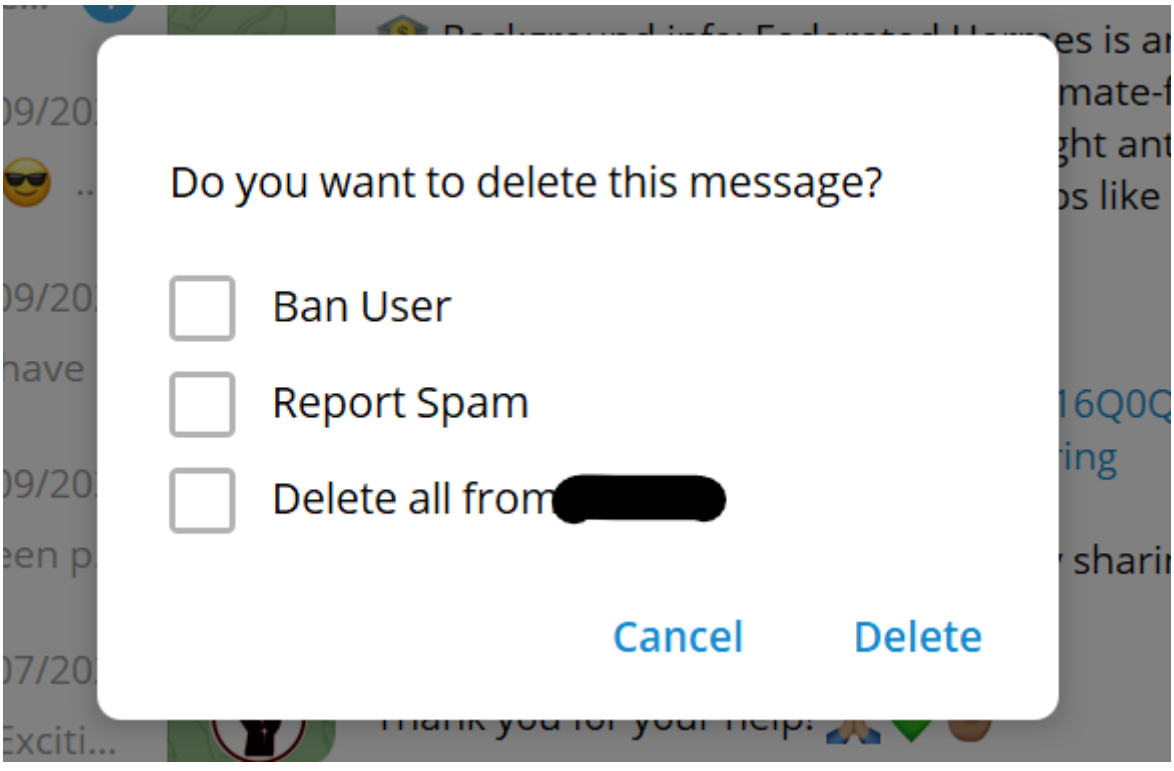
- **On a phone** - tap to the right of their name on the words 'X joined the group via invite link'.
- **On a computer** - right click on the words 'X joined the group via invite link'.



4. Select "delete"



5. Select the 3 tickboxes: Ban user, Report spam and Delete all



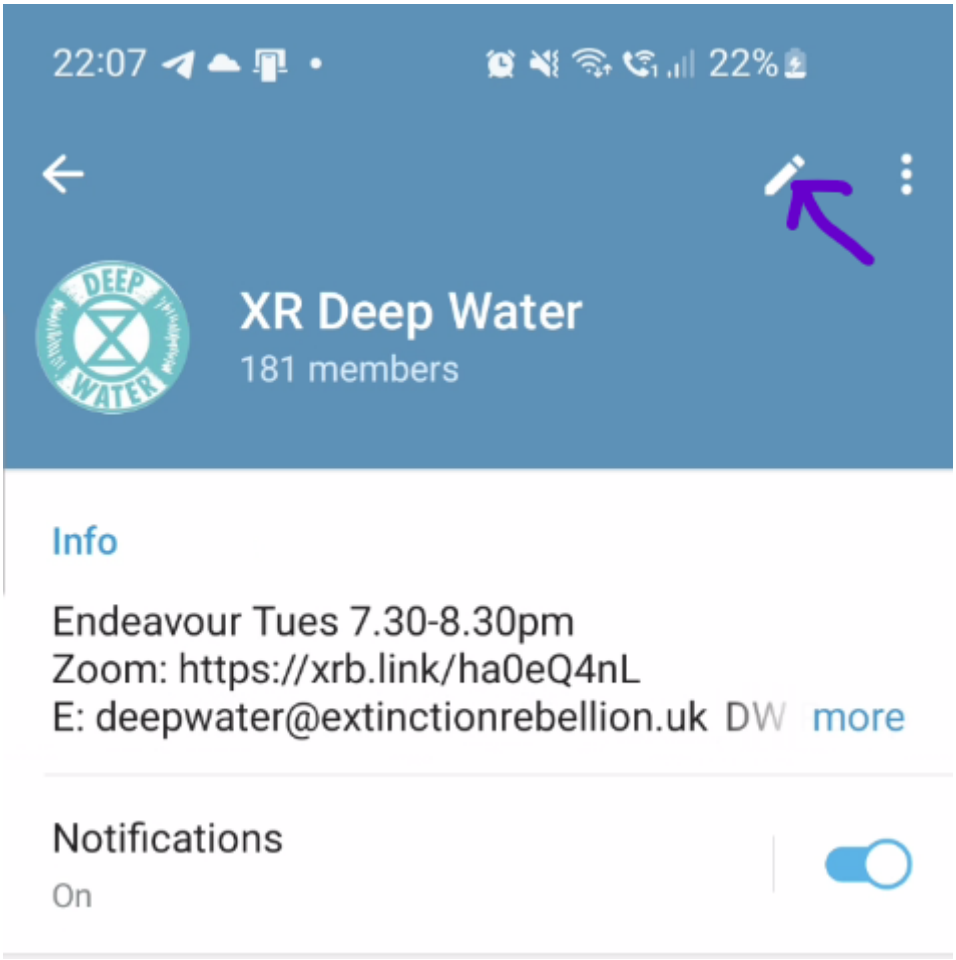
If you simply search for a spammer from the member's list and block and report them from there, that only blocks / reports the spammer for yourself rather than the whole group and it also doesn't delete any spam messages they may have posted.

6. Revoke the current invite link

You can revoke the current invite link so more spammers can't use it and create a new invite link to be shared with only trusted rebels

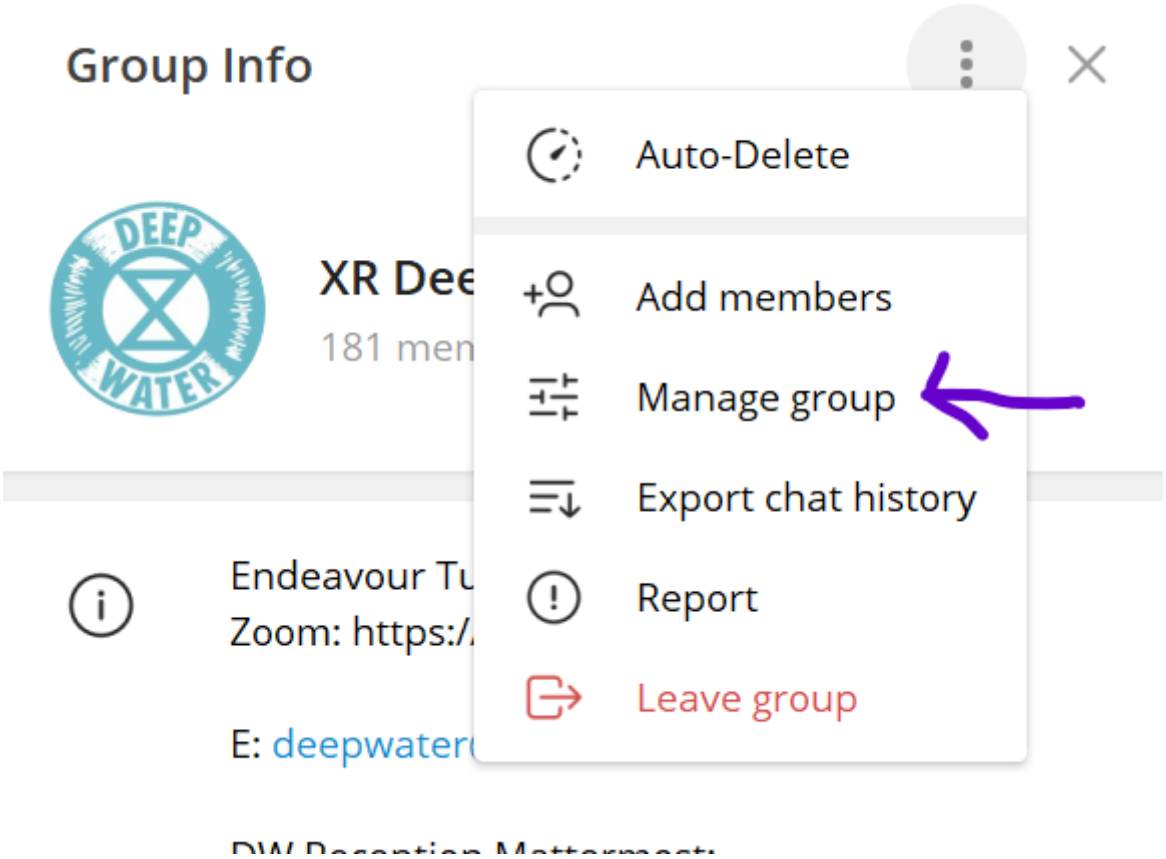
On a phone:

- 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'
- Go to 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

7. To change permissions to prevent more spammers adding more spammers

So spammers can't add more spammers/bad agents to your group, select 'Permissions' and switch off 'Add Users'.

Messaging Apps: Broadcast Channels

Broadcast-only channels are for sharing key information to your group and supporters, to mobilise people to attend actions, events and training.

This page offers guidance in setting up, running, and creating messages for a broadcast channel.

Setting up a broadcast channel

- Consider setting up a broadcast channel only if there's a strong need for it. Does your team have the capacity to moderate the space and a process in place to generate content for the channel?
- Be aware of the channel's place in the wider movement and the issue of comms overload. Less is more. Encourage your group to follow the Rebellion Broadcast (for actions, events and movement news) and the Rebellion Broadcast (for talks, training and workshops) to help reduce communication overwhelm.
- Set up a 'Request Channel', for people to request messages to be sent out on the broadcast. This can be via a dedicated email address, DM-ing the Broadcast coordinator, or having an open channel (typically on the same platform as the broadcast) where people can put their requests. The system needs to be communicated to your group so it's clear how to use it.
- Manage expectations by giving criteria for what will get broadcast.
- Assign a coordinator to process messages.
- If multiple people are involved in running the channel, set up a private chat for the editing team, where you can draft, review and approve messages before they go out.
- If you are using Telegram, consider syncing it to Mattermost via a bridge to serve both platforms.

Using a broadcast channel

- Limit the number of messages and have a balance of content. Plan a flow of broadcast comms that is mindful and doesn't overwhelm the chat - stagger them over a period of time in the run up to an event.
- Have a broadcast communication plan and build up to events as part of a wider strategy.

- Leave time for your message to land- this is usually 2 weeks, 1 week minimum to promote an event. Last minute calls-to-action do not necessarily reach everybody and can be counterproductive.
- Don’t share messages elsewhere before they’ve gone out on your main broadcast channel to reduce the likelihood of mistakes being sent out. It can also be confusing for people to receive different versions of the same info.
- Top tip: if you're using Telegram, you can share the link to a Telegram message. Right-click on the post and click *Copy Link*, then post this link in your chat. This can help steer folks back to the main broadcast channel.

Documents

Which document platform to use

The XRUK Cloud

A safer and secure option is the XRUK Cloud

- Private & Secure – we host it in Switzerland
- By default, files are owned by a group not an individual - so no data loss when individuals step back
- All the usual features from Google/Microsoft (backups, auto-save, document format compatibiilty, etc)

Read more about why the XRUK Digital circle recommends using the XRUK Cloud here.

More info on how to start using the the XRUK Cloud here.

Google and Microsoft

Google Docs enables you to share information in a fluid and integrated way with others, including taking comments and suggestions. Remember to make **final versions that you are sharing "View Only"** so they can't be changed. Plus an added layer of security is to change the very ending of the URL after the final / to **/preview**. This is normally instead of /edit. This also makes viewing the document look 'cleaner' to the people you are sharing it with.

However, it has a lot of drawbacks (If you don't pay for the product, you are the product):

- Even if you have a local group gmail account, by default docs will be created in your personal account.
- Managing Google/Microsoft shared files and folders can quickly get out of hand.
- If you step back from XR, your group will lose access to potentially years of work.
- Google and Microsoft will hand your data to the authorities if requested. In extreme cases, they could suspend your account without notice.

Cryptpad

Cryptpad is a shared document app similar to Google Docs but far more secure, especially if used with a password (but it is not as user friendly). You can use Cryptpad for any restricted information

like plans or lists of participants, and always save these with a password. The XR cryptpad is hosted and run by XRGlobal, and can be accessed through the XR Hub.

Top tips for clear and coherent docs

- Make the name of the doc clear and different to other docs.
- Add the aim, date and key information at the top, to make it clear to everyone reading what the doc seeks to achieve and prevents docs being circulated that spread misinformation.
- More information on creating accessible documents here.
- Keep it short - rebels are overloaded with information!
- Do not include spicy information or implicate organisers.

Style Guide

When information is consistent in visual appearance, language and formatting, it is easier to understand and disseminate. It becomes instantly recognisable as the XR voice and it fits within the wider context of the movement, lending it strength.

Design

See the Design Programme for fonts, logos, colours, images, icons etc.

Be consistent in the name and image used for the event/action across all platforms.

Accessibility

Consider accessibility: It is key in reaching as many people as possible and growing our movement. Mention where people can find out more about physical accessibility.

Write for a teenager for whom English is second language. Keep sentences short and use plain English, not academic terminology. Don’t assume knowledge, for example make clear what abbreviations stand for.

See Accessible documents for advice on making your communication accessible, including for considering colour blindness and dyslexia.

Banner Images

E.g. for social media posts and messaging apps

- Use Fucxed Caps (the main XR font).
- Colour scheme: use colours from the XR Design Programme (this can include different shades of one colour).
- Limit the words in a visual banner. Put a short title only into the image. Text in images is not fully accessible as it cannot be read by screen reader technology. Keep the design clean and readable.
- Use one font size for the banner design (or two max). Keep it simple and clear.
- Centralise the text in the image.

- Use a consistent margin around the edge of the image for breathing space, so that the text or logo doesn’t sit on the edge of design.
- Check the image and text is in focus. Do not use it otherwise!
- Avoid too many overlays of images or text as it can be overwhelming.
- We advise using black or white text on a background colour for contrast and clarity. Make it clear.
- Consider dimensions (see below).

Spelling and grammar

This may not matter for some people, but for the rest, it is enough for them to abandon reading our posts. And for many it’s simply good manners.

When writing anything as XR, avoid:

- Spelling errors
- Grammar mistakes

Commonly misspelt words:

- Citizens’ Assembly; plural - Citizens’ Assemblies
- People’s Assembly; plural - People’s Assemblies
- De-escalation
- Nonviolence, nonviolent
- Wellbeing
- Campsite
- Any more (with a space)
- X-year-old
- XRUK (the hive and its subcircles, as opposed to "XR in the UK", which includes all the nations, regions, local groups, community groups, and so on)

Know the difference between:

- Their, There and They’re
- It’s and Its
- Lose and Loose
- To, Too and Two

Use apostrophes accurately or don’t use them at all.

Time

- Use a 24h clock or specify am/pm or AM/PM
- Include a colon, e.g. 17:00 or 05:00pm

Messaging app messages

General

- See the Rebellion Broadcast or Movement Broadcast Telegram channels for examples of well-formatted messages.
- Keep messages short. Link out to further information.
- For broadcast posts write like you are XR, not your individual voice.
- A broadcast post will get shared across different platforms so make sure the context is included (date/name of event) and that it says XRUK rather then ‘we’ or it won’t be clear where it’s from.

Headings

Put the message title in **CAPS and in bold**. Simply putting the title in bold or framed by emojis doesn’t translate well when it’s shared across channels, e.g. from Telegram to Signal or phone to laptop view.

Links

- Use XR’s link shortener to make links shorter. You’ll need an XR Hub account to create XR short links. If you don’t have one use TinyURL.
- Put weblinks on the next line after the text/colon: this is for accessibility as it’s easier to read.
- Don’t use direct (embedded) links on Telegram, share the full hyperlink instead, as messages are often shared-on to other platforms that may not support linking.
- Close linked windows (the cross in top right corner of the message) to reduce the message length and make a neater visual.

Images

- Don’t use an image unless it’s a good one, clear & dynamic with high contrast.
- The dimensions for using an image on Telegram are 1920 x 1005 (the same proportions as a Facebook event header)
- Keep it simple. One image is advised for the best effect, ideally in landscape. If you don’t have a strong image then no need to add one.
- Attach an image to the message, rather than posting it before on its own. This prevents it from getting lost when messages are forwarded.
- In Telegram, if you have multiple images you can attach them straight to the message and they will automatically form a grid.
- A general rule of thumb is max 5 images per collage, otherwise it risks becoming cluttered. A single image can sometimes be more striking.
- Aim for clear images (remember most people will view it on their phones).

- To make graphics (like the Open Call image below) use Aktavisda.

Example images:

Emojis

- Limit the use of emojis- less is more!
- Don’t frame a message title with emojis or use emojis at the end of a line. The emojis often jump lines when the message is shared to different devices or platforms (Android or iPhone, Signal or Telegram, phone or computer) and can end up looking messy.
- Just use one emoji at the start of the title, if you’re going to use them, and try to colour-coordinate with the header image.
- Use one space between image and emoji.
- Consider inclusivity when using emoji skin colours for hands etc. If you want to find more Telegram emojis including additional skin tones check out emojipedia.

Lists

Lists made up of complete sentences or following straight on from a heading:

- Each line should start with a capital letter.
- Each line should finish with a full stop.
- List should consist of 3 points or more.

- Try to keep each line a similar length.

Lists consisting of words/short phrases:

- require a lead in line followed by a colon
- can begin with a lower case letter
- do not require full stops

In a list laid out as a complete sentence, we:

- can use lower case,
- should use a comma at the end of each line, and
- end with a full stop.
  (the 'and' shown here isn't always necessary)

Numbered lists:

1. These should only be used if giving instructions that must be followed in a specific sequence.
2. Each line is treated as a complete sentence with a capital letter and full stop.
3. Ideally the points will flow on one after another, e.g. if first few points start with a verb it can be jarring if the next point does not.