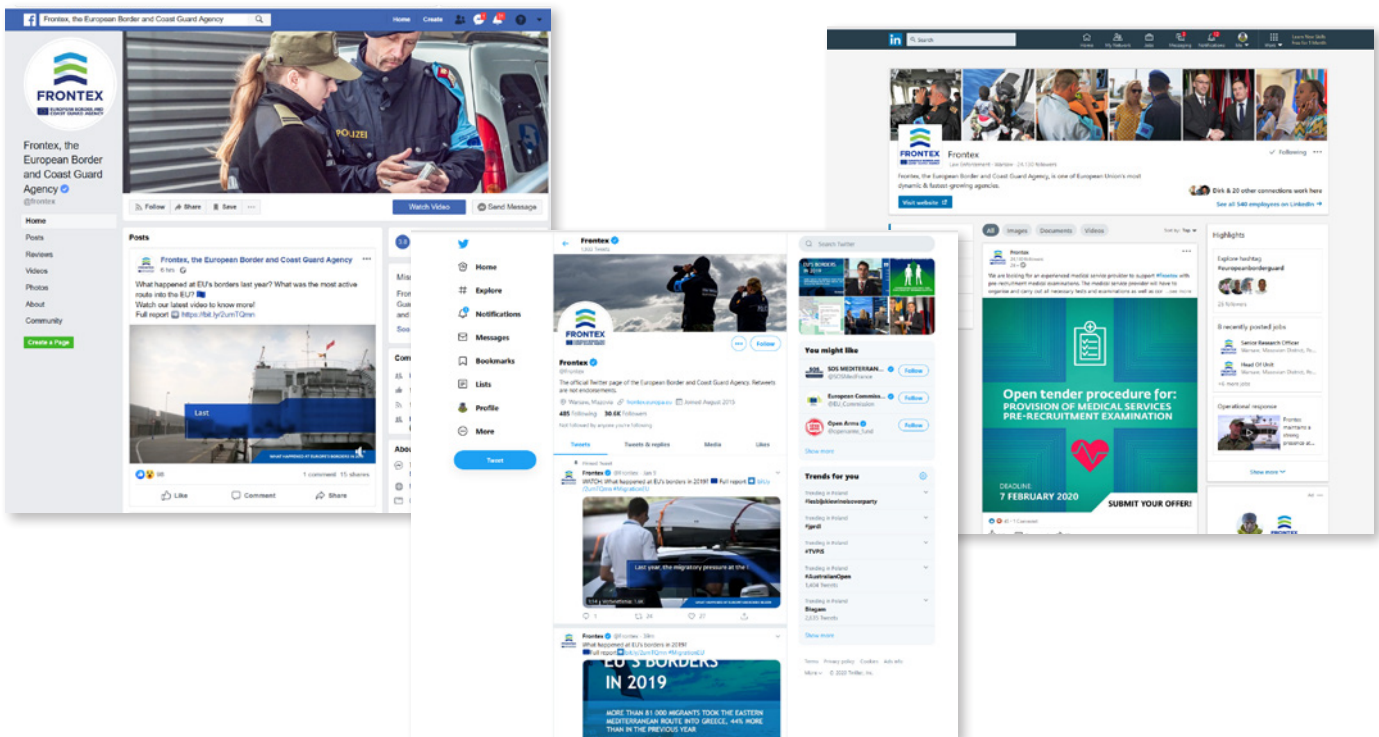


FRONT_{EX}



GUIDELINES FOR SOCIAL MEDIA USE

GUIDELINES FOR SOCIAL MEDIA USE



Social media platforms allow people to create and share information directly with millions of users. They can use a variety of formats, including text, pictures, audio and video. They are used to share content, opinions, information, promote discussion and build relationships.

Popular social media platforms, such as Facebook, LinkedIn, Twitter, YouTube, Flickr and Instagram, have become important outreach and communication tools not only for individuals, but

also for the private and public sectors. Messaging services such as Messenger, Telegram and WhatsApp are largely used to share opinions and information among individuals and groups.

While Frontex staff and persons involved in the activities coordinated by the agency should enjoy sharing knowledge and maintain professional or personal contacts with their colleagues online, we also have a duty to protect the agency's reputation.

Today it takes more than a press release to communicate effectively. This is why Frontex is active on a variety of social media channels.

We are open and transparent and our goal is to explain what we do and why we do it to both external and internal audiences. We encourage you to share the content we publish, to send us your stories, photos and testimonials and to let the Frontex Media and Public Relations team know about any events or activities that could be promoted online.

We do not want to limit your freedom of expression, but we care how an improper post could affect Frontex and its stakeholders. This is why we would like to provide you with some guidelines for the personal and professional use of social media.

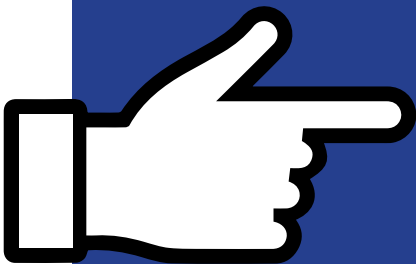


You are responsible for content you publish on social networking sites, blogs or elsewhere online. Your actions online should reflect the core values of the European Union.

Avoid any behaviour that could discredit yourself or Frontex, the European Border and Coast Guard Agency.



Remember that your posts will stay online forever and may affect the reputation of Frontex, as well as your own. These rules and simple tips will help you use social media in your professional and personal life.



As a general rule, only the Executive Director, spokespersons and other authorised staff are entitled to speak on behalf of the European Border and Coast Guard Agency.

Official social media accounts of Frontex, the European Border and Coast Guard Agency, are managed by the agency's Media and Public Relations (MPR) Office.

SOCIAL MEDIA RULES AND TIPS

Rules

No classified, sensitive and protected information

Do not post information marked as classified, sensitive or limited, or that protected by a confidentiality clause within a contract. Do not share notes, emails (including attachments) and other information from internal meetings. If in doubt, talk to your supervisor or the Frontex Media and Public Relations Office.

Work-related information should stay off social media

We strongly discourage you from discussing work-related details online unless it is information already made public or approved for public release. Do not post photos or information from your deployments and missions with Frontex. Never tag yourself, nor other people such as colleagues or participants, in operational areas and do not disclose the name of the agency, the name of the operation, location, duration, equipment nor any other details that could compromise the activity or national authorities.

Use your professional judgement before you post

You are responsible for what you post. The same rules apply if you post something on Twitter, comment under an article or photo in LinkedIn or express your opinion in a closed Facebook group. Even if deleted, a post can still be retrieved.

Differentiate between opinion and official information

When you post something related to our activities, make it clear that you express your personal opinion, not that of Frontex.

Respect applicable law and copyrights

On social media, use your own name or a chosen alias. Do not create fake accounts. Do not disseminate or create fake news or post materials protected by copyright without the written permission of the copyright owner. Do not use the Frontex logo without the written permission from the Media and Public Relations Office.

Tips

Separate private from professional

On social media, do not reveal details of your employment, including exact tasks, personal information about your supervisor and other details of your work. On services such as LinkedIn, keep your profile general and only include information that is already public. When you travel for work, do not reveal details of locations and tasks and do not tag yourself and other people when staying in hotels, restaurants or other facilities. Think twice before posting photos from business trips. These could put you or others in danger.

Pay attention to language

Do not post obscene, hateful or abusive content and show respect for the opinion of others. Even if you write in your own capacity, you might be regarded as a representative of Frontex.

Review your privacy settings

Maintain and review privacy settings on your social media accounts, change passwords regularly and consider using two-factor authentication where available. Be careful about the personal information you share. Read the rules described in the terms of use and privacy policy of the social media you use.

Remember: when you join a social network, you sign a contract with that provider accepting the terms of use and services.

Help us explain what Frontex does

When you see someone make factual errors about Frontex on social media, help us correct it. We will help you formulate a response or clarify the information on the institutional level. Please report such issues to HoO.MPR@frontex.europa.eu

Separate facts from fakes

Social media can be used to spread false information. When sharing or reading an article or watching a video, check the source and the author to protect yourself against disinformation. If you need help, please contact

HoO.MPR@frontex.europa.eu

MEETINGS AND CONFERENCES



At Frontex, we want to explain our activities and mandate to the general public and often use social media to talk about the participation of the agency's staff in conferences, meetings and study visits.

Remember

If you take part in a meeting or conference that your managers would like to communicate on, get in touch with Frontex's social media and editorial team (HoO.MPR@frontex.europa.eu) ahead of time. Send us photos and short information about the meeting.

Be aware that any information you present at conferences may be photographed and shared. **If you present sensitive/limited, classified or protected information make sure to inform your audience about the rules regarding the distribution of that content.** If you need help, please contact security at HoS.SEC@frontex.europa.eu

Prior to attending a meeting, always ask the organisers if media are going to be present or whether the organisers intend to publicise your participation on social media.

Rules

Frontex is a law enforcement agency and field deployments should be seen as police missions. Do not disclose any information about the purpose of your trip, exact location, participants or other details that might compromise the aim of your mission.

Tip

Remember that if you post photos from your missions, even after working hours, your business trips may be perceived as leisure activities at the taxpayer's expense.



Franca

12 December at 12:45

My name is Franca and I am working as fingerprinting expert on Lesvos as part of Frontex operation Poseidon. I am proud to be part of #Frontex #Poseidon and deployed in Greece!
<https://frontex.europa.eu/media-centre/our-officers/>



YES




Francis

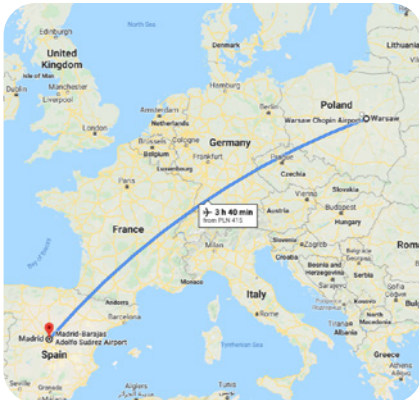
4 December at 16:45

After a hard day with @Frontex in #hotspot on #Lesvos now it's time for a pint! #operationPoseidon



NO

Casper was  travelling to **Madrid, Spain** from **Poland - Warsaw**
07 May at 04:05 Warsaw



YES



Casper is in **Hilton Madrid** with **John Smith**
07 May at 04:5

Another business trip with Frontex! #Frontex #operationIndalo



NO

EXPRESSING POLITICAL VIEWS

Everyone is entitled to their own political views and opinions. However, we encourage you to be careful with expressing your political views on social media. Nowadays no one is anonymous and openly criticising a political formation, institution or government policies, especially if you are in a managerial position, may reflect adversely on your position as an employee of a European Union agency.



I disagree with the current policies on...
and think that this goes against EU's values

YES



I hate that government! They are a bunch of liars!

NO

IMAGES

A picture is worth a thousand words. When you post photos online, make sure they do not reveal any sensitive information, such as personal data you would not want everyone to see.



Rules

Do not take photos of anybody unless you have their explicit permission, this includes your colleagues, but also local residents and migrants.

Do not take photos of border crossing points, police stations, coordination centres and technical equipment without authorisation from the relevant authorities and Frontex.

Tip

Be cautious when taking photos and, if in doubt, double check with MPR before publishing them. Sometimes objects visible in the background of your picture (flipcharts, whiteboards, computer screens or documents on a desk) can expose sensitive or classified information.

PROTECT YOURSELF AGAINST DISINFORMATION

Social media can be used to spread false information to cause confusion or to lead the target audience to believe a certain narrative. Disinformation spreads online faster than real news and can be amplified by bots or people using false identities. Left unchecked, these false narratives can influence political views, disrupt campaigns, encourage extremism and

undermine the democratic discourse. The European Union is actively countering disinformation online through a variety of initiatives, but there are a few simple steps that social media users can follow to protect themselves against disinformation.

(Source: European Commission)

1. Check the source

Are you familiar with the news outlet sharing the information? Does the look or feel of the outlet resemble a well-known website but is not quite the same? This could mean the source is unreliable or deceptive.

2. Check the author

If an author or journalist is credible, you should be able to track their previous work and find which organisations they have worked for. You should also be able to find other articles or publications they have written. Keep in mind that sometimes an "online expert" may not really be an expert in the subject. There is a difference between a specialist and someone obsessed with conspiracy theories.

If you see a social media account posting hundreds of times a day, especially on Twitter, and frequently at suspicious times like at 4 AM, it is likely to be a bot. Other red flags include language or syntax errors and little or no engagement in real conversations.

3. Check the content

Is the story you want to share being covered by traditional media, like newspapers or broadcasters? Does the story match the information put out by public authorities and institutions or NGOs? Remember, credible media outlets have clearly defined reporting standards and the news that they present is balanced, with attributed sources, and has context.

4. Check the pictures and videos

"Seeing is believing" is no longer a given. Sometimes old images are used in different contexts or are completely fake. To verify whether an image is real, you can always try to track back to its original source or use various "online reverse image tools." Keep in mind that disinformation technology is constantly evolving as exemplified by the emergence of manipulated videos such as "deepfakes".

5. Report

If you think that an account is spreading disinformation, report them or the post to the social media platform. *(Source: European Commission)*

Rules

Any exchange of work-related information must be done through secure email systems.

Do not create or use discussion groups, either closed or open, to exchange work-related information with your colleagues.

Do not reveal details about Frontex's internal systems, assets, operations in your job description on social networking sites, such as LinkedIn.

TIPS

Review your privacy settings. We recommend setting security options to allow visibility to "friends only".

Be aware of cybercrime, such as identity theft, phishing, and spam offers. Do not share your personal information, including financial data, on social media.

Be cautious when enabling geotagging on mobile or other location-based apps because they could potentially create personal and operational security risks.

Use strong and long passwords and consider changing them regularly to minimise the risk of data breaches.

Do not use the same password for all your accounts.

On social networking sites, use two-factor authentication, if available.

IN SHORT:

Refrain from any on-line behaviour that may harm your professional position and Frontex.

- Do not post obscene, hateful or abusive content.
- Use appropriate language and show respect for the opinion of others.
- Never discuss protected, sensitive or classified information.
- Pay attention to the rules and regulations regarding the use of social media.
- Do not speak on behalf of Frontex on social media.
- Do not discuss work-related issues.
- Do not disclose information that has not already been made public by Frontex.
- If you take part in online discussions, make clear that the opinions you post are your own.

These guidelines apply to all social media activities and messaging applications, including closed groups on Facebook and WhatsApp. Do not assume that information you post in a closed group will not reach a wider audience.

Disclosure of classified, sensitive or limited information related to the agency or that jeopardise its reputation could lead to disciplinary actions (Staff Regulations, Article 12).

1. Can I identify myself as a Frontex employee on social media?

Yes, you can. You can link to the official social media accounts of Frontex in your profile. However, do not disclose detailed information about your role, your position, personal details of your supervisor and any other information that is not public or might be sensitive.

2. Am I allowed to share information about Frontex online?

You are allowed to share any official communication from the agency's website and social media channels that has already been published on Frontex website or any of its social media channels. You are also allowed to share news articles related to the work or activities of Frontex provided the information they contain is actual and the source is credible. Avoid sharing articles expressing controversial opinions as this might be taken as endorsement.

3. I have seen someone post false information about migration on Facebook. Can I correct it and post a reply?

Unless authorised, you are not entitled to speak on behalf of Frontex. If you see false or misleading information posted about Frontex, or any activity related to the work of the agency, get in touch with mpr@frontex.europa.eu – our team will analyse the situation and, if necessary, contact the author.

4. I am taking part in a conference as part of a Frontex delegation. Can I tweet about my participation?

That depends. If the organisers of the conference allow it and you have the approval of your supervisor and Frontex Press office. You can say that you take part and represent the agency without providing details. You may also share information about the event with the MPR office, which may want to publicise it via Frontex social media channels.

5. I am deployed or on mission in Greece. After work, can I share photos from a beach or a restaurant?

During your deployment/mission, conference or meeting you represent Frontex. Use your own judgement. Do not make your deployment seem like a holiday. Do not post photos of yourself in your uniform, with a Frontex armband, with colleagues who do not agree to be photographed and never with alcohol. Don't tag yourself and others in restaurants or hotels.

Other questions?

Get in touch with HoO.MPR@frontex.europa.eu

