

Online Safety Toolkit

A practical guide for migrants and refugees

About this guide: This guide is written in simple language so it is easy to read and easy to translate. It may be freely shared, printed, and distributed.

Online Safety Toolkit	1
QUICK REFERENCE CARD	1
If something goes wrong — who to call.....	1
Keeping your password safe	2
Have your own personal email account	2
Two-factor authentication (2FA)	3
Being safe on social media.....	3
Do not share personal information online	4
Online harm can reach you across borders	4
Accessing donated data and devices.....	5
How to translate documents	5
What to do if something goes wrong	5
Quick comparison of messaging apps	6
WhatsApp — staying safe.....	6
Telegram — what you need to know	7
Signal — the most private option.....	8
Using your phone safely at borders and with authorities	9

QUICK REFERENCE CARD

Print this page and keep it somewhere safe.

Passwords Long, unique password for every account. Use a password manager. Never share passwords.	Your own email Have an email only you use. Keep recovery details written down somewhere safe.
Two-factor (2FA) Turn on 2FA on all accounts. Use Google Authenticator or Authy app.	Social media Set to private. Never post your location or documents. Think before you post.
Personal info Never share passport, ID, address or case number online. Beware of scams.	Messaging apps Use Signal for sensitive messages. Check WhatsApp privacy settings. Be careful on Telegram.
Online harm Harm can reach you across borders. Screenshot threats and report them to the platform.	At borders Back up your phone before travel. You can turn it off. Know your rights.

If something goes wrong — who to call

Who	How to reach them
Emergency (police, fire, ambulance)	999
Non-emergency police	101
Migrant Help — free 24/7 helpline	0808 8010 503
ClearCommunityWeb	www.clearcommunityweb.co.uk
Screen Share UK	www.screen-share.co.uk
The Cyber Helpline	www.thecyberhelpline.com
Victim Support	www.victimsupport.org.uk
Report Fraud	www.reportfraud.police.uk

Keeping your password safe

Your password is like a key to your home. If someone has it, they can get into your accounts — including your email, bank, and government services.

1. **Long password.** Use a long password — at least 12 characters. Use a mix of words, numbers, and symbols. Example: BlueSky!River#2024
2. **Different passwords.** Use a different password for each account. Never reuse the same password.
3. **Password manager.** Use a password manager app to remember all your passwords safely. Free options: Bitwarden, Google Password Manager.
4. **Never share.** Never share your password — not with friends, family, or anyone who says they are from a government or company.
5. **Recovery details.** Write down a recovery email and phone number for each account and store them somewhere safe offline.

Important: If you lose access to your email, you may not be able to receive letters from the Home Office, courts, or other services. Always keep your recovery details up to date.

Have your own personal email account

It is important to have an email address that only you use. Do not share an email account with family members, friends, or anyone else.

Free email services: Gmail (Google), Outlook (Microsoft), or ProtonMail (extra private).

Watch out: If you share an email, another person could change your passwords, read your documents, or speak on your behalf without your knowledge.

Two-factor authentication (2FA)

Two-factor authentication adds an extra step when you log in. Even if someone knows your password, they cannot get into your account without a second check.

Think of it like a door with two locks. Even if someone has one key, they still cannot get in without the second.

1. When you log in, you will be asked for a code sent to your phone by text message, or from an app.
2. Turn on 2FA in the Security Settings of your email and all important accounts.
3. A free app called Google Authenticator or Authy can generate your codes — this is safer than text messages.

Tip: Save your backup codes somewhere safe (printed or written down) in case you lose your phone.

Being safe on social media

Social media can connect you with family and community — but it can also be used against you. Be careful about what you post and who can see it.

1. Set your profile to private so only people you approve can see your posts.
2. Do not post information about where you are or where you are going.
3. Do not post images that show your address, documents, or ID cards.
4. Be careful about accepting friend requests from people you do not know — even if they say they are from your country.
5. Remember: posts you made years ago can still be found and used by others, including authorities.

Remember: Immigration authorities in some countries can check your social media. Think carefully before you post anything about your location, plans, or opinions about governments.

Do not share personal information online

Personal information (also called 'personally identifiable information') is any information that can identify who you are.

Never share online:

- Full name and date of birth together

- Passport or visa number
- National ID number
- Home address
- Fingerprint or photo of your face used for ID

Be careful with:

- Your phone number
- The city you live in
- Names of your children
- Which asylum centre or hotel you are in
- Your case or reference number

Scam warning: If someone online offers to help with your visa, housing, or benefits and asks for your personal details — this may be a scam. Only share personal information with official organisations you can verify.

Online harm can reach you across borders

The internet has no borders. Online harm does not stop when you move to a different country.

1. People or governments in your home country may try to monitor your accounts or contact your family to find out where you are.
2. Stalkerware is hidden software that someone may have put on your phone to track you. If you think this may have happened, contact a support organisation.
3. Be careful of online groups that seem friendly but may be gathering information about migrants or refugees.
4. If you are being harassed or threatened online, take screenshots, report it to the platform, and tell a support organisation.

Protect yourself: You can use a VPN (Virtual Private Network) to make it harder for others to track your internet activity. A free option is ProtonVPN.

Accessing donated data and devices

Many charities and organisations offer free or low-cost phones, SIM cards, and internet data to migrants and refugees in the UK.

You may need to be referred by an organization who supports you to be eligible.

ScreenShare

The only national charity dedicated to supporting Asylum Seekers and Refugees with access to devices, sims and skills development.

<https://www.screen-share.co.uk>

Community Tech Aid

A charity providing access to donated laptops, sims and mobile phones to people based in Lambeth and Southwark. A referral from an organization is required.

<https://www.communitytechaid.org.uk>

ClearCommunityWeb

Digital skills support and safety awareness across Croydon, Lambeth, Southwark and Bromley

<https://clearcommunityweb.co.uk>

Sims

- **O2 Store Databanks:** You can walk into participating [O2](#) stores to request free mobile data, texts, and minutes if you are struggling with data poverty.
- **Virgin Money Stores:** Participating [Virgin Money PLC](#) locations offer O2 SIM cards with 20GB of monthly data for up to six months

Safety tip with donated devices: Before using a phone or laptop given to you, ask someone you trust to check it, or do a factory reset to remove any old data or software from the previous owner.

How to translate documents

You may receive letters or documents in English that you need to understand. Here are free ways to translate them.

1. Google Translate (translate.google.com) — take a photo of a document and it will translate it. Works in 100+ languages. Free.
2. Microsoft Translator — similar to Google Translate, also free.
3. Your phone's camera — both iPhone and Android phones can translate text you point your camera at, in real time.

4. For important legal documents, ask for a professional or certified translator — your support organisation may be able to help with this for free.

Important: Machine translation (like Google Translate) is good for understanding, but it can make mistakes. Do not rely on it alone for important legal decisions. Always ask for help from a professional when the document is about your case.

What to do if something goes wrong

If you have a problem online — such as someone accessing your account, threatening you, or scamming you — do not panic. There is help available.

1. Change your passwords immediately if you think someone has accessed your account.
2. Take screenshots of anything that happened — messages, threats, or suspicious activity.
3. Report it to the platform (Facebook, Google, etc.) using the 'Report' button.
4. Contact a support organisation — see below. They can help you even if you do not speak English well.
5. If you are in danger, call 999 (UK emergency services). For non-emergency police: call 101.

Quick comparison of messaging apps

Feature	WhatsApp	Telegram	Signal
Encrypted by default?	Yes	No — only in Secret Chats	Yes — always
Stores messages on servers?	Encrypted backups	Yes (regular chats)	No
Best for	Everyday family contact	Public channels and news	Sensitive conversations
Free to use?	Yes	Yes	Yes
Who owns it?	Meta (Facebook)	Telegram (private company)	Signal Foundation (non-profit)

Simple rule: Simple rule:

- Use Signal for anything sensitive or private.
- Use WhatsApp (with correct settings) for everyday family contact.
- Be very careful with Telegram — use Secret Chats only for anything private.

WhatsApp — staying safe

WhatsApp uses end-to-end encryption for all messages. This means only you and the person you message can read them — not WhatsApp, not governments. But you still need to check your privacy settings.

How to do a WhatsApp Privacy Checkup

Open WhatsApp → Settings → Privacy → Privacy Checkup. Then check each of these settings:

Setting	What it means	Recommended
Profile photo	Who can see your photo?	Set to: My contacts
Last seen & online	Who can see when you were last online?	Set to: Nobody
About	Who can see your 'About' description?	Set to: My contacts
Status	Who can see your status updates?	Set to: My contacts
Read receipts	Blue ticks that show you read a message	Consider turning off
Groups	Who can add you to groups?	Set to: My contacts
Live location	Are you sharing your location with anyone?	Check and stop sharing
Blocked contacts	Anyone harassing you can be blocked here	Review regularly

More important steps

1. Turn on two-step verification: Settings → Account → Two-step verification → Enable. Add a PIN and an email address.
2. Check linked devices: Settings → Linked Devices. Remove any device you do not recognise.
3. Turn on disappearing messages for sensitive conversations: open the chat → tap the name at the top → Disappearing Messages → 24 hours or 7 days.
4. Be careful in large WhatsApp groups — anyone in the group can screenshot your messages or see your phone number.
5. Never send photos of documents, passports, or ID cards over WhatsApp, even to people you trust.

Important about groups: If you are added to a group by someone you do not know, leave it immediately. Some groups are used to spread false information or to identify migrants and refugees.

Tip: Use the 'View Once' feature when you must send a sensitive photo — the image disappears after the person views it once.

Telegram — what you need to know

Telegram is very popular in many communities. However, it is NOT fully end-to-end encrypted by default. Regular chats are stored on Telegram's servers and could be accessed by others.

1. For private conversations, always use a Secret Chat. Go to: New Message → New Secret Chat. Secret chats are end-to-end encrypted and not stored on Telegram's servers.
2. Set a passcode lock on the Telegram app: Settings → Privacy and Security → Passcode Lock.
3. Turn on two-step verification: Settings → Privacy and Security → Two-Step Verification.
4. Check who can see your phone number: Settings → Privacy and Security → Phone Number → set to 'Nobody'.
5. Turn off the 'People Nearby' feature: Settings → Privacy and Security → People Nearby. This feature can reveal your location to strangers.
6. Check active sessions: Settings → Privacy and Security → Active Sessions. Remove any sessions you do not recognise.

Large public groups: Telegram has very large public groups and channels. Anyone can read these — including people you do not want to see your messages. Be very careful what you say in public groups.

Important: Telegram is often monitored in certain countries. If someone from your home country is pressuring you to join a Telegram group, speak to a support organisation before responding.

Signal — the most private option

Signal is considered the most private and secure messaging app available. It is used by journalists, lawyers, and human rights workers for this reason. All messages are end-to-end encrypted by default — including calls and group chats.

1. Download Signal for free from the App Store (iPhone) or Google Play (Android). It is free and open source.
2. Turn on disappearing messages for all chats: Signal Settings → Privacy → Default Timer. Set to 1 week or less for sensitive conversations.
3. Enable screen lock: Signal Settings → Privacy → Screen Lock. This stops someone picking up your phone from reading your messages.

4. Turn on screen security to stop screenshots being taken of your Signal chats: Settings → Privacy → Screen Security.
5. Use 'Note to Self' as a private place to store important notes — only you can see this.
6. You can make encrypted phone and video calls on Signal too — these are private and cannot be listened to.

Recommended: If you need to share sensitive personal information — for example with a lawyer, support worker, or family member — use Signal. It is the safest option for these conversations.

Using your phone safely at borders and with authorities

Border officers in many countries — including the UK — have the power to ask you to unlock your phone or hand it over for inspection. This can feel frightening. Knowing what to expect and preparing in advance can help protect you.

Before you travel — prepare your phone

1. Back up everything before you travel. Use Google Drive, iCloud, or a computer to save your photos, contacts, and important messages.
2. Consider logging out of sensitive apps before you reach the border — including social media, messaging apps, and email. You can log back in once you are through.
3. Delete any content you would not want an official to see — including messages, photos, or apps. Remember: things stored in the cloud may still be accessible if you are logged in.
4. Note down important phone numbers (lawyer, support worker, family) on paper, in case your phone is taken.
5. You may want to turn your phone off before reaching a border checkpoint. This means a fingerprint or Face ID alone cannot unlock it — the passcode is required when a phone is restarted.

Your rights at the border

1. In the UK, border officers can ask to search your phone under Schedule 7 of the Terrorism Act 2000. You do not have to be suspected of a crime for this to happen.
2. If you refuse to give your passcode at a UK border, you can be arrested. This is different from other searches — the law here requires cooperation.
3. You have the right to ask why you are being searched and to be told what your rights are. Stay calm and be polite.
4. You have the right to contact a lawyer. If you are detained, ask to speak to a legal representative before answering questions.

5. If your phone is taken, ask for a receipt — a written note of what was taken and when.

During a stop or encounter with police or officials

1. Stay calm. Do not argue. You can say 'I do not consent to this search' — this does not stop them, but it means you have made your position clear.
2. Do not lie to officials — this can seriously affect your case. It is better to say 'I do not want to answer that question without a lawyer' than to give false information.
3. If you are able to, try to remember details of what happened — the time, location, what the officer said, and their badge number. Write these down as soon as you can afterwards.
4. Tell your support worker or lawyer about any border searches or stops as soon as possible, especially if anything was taken.

Important: This information is general guidance only and not legal advice. Laws differ between countries and can change. If you are worried about a specific situation, speak to a lawyer or contact Migrant Help on 0808 8010 503 before you travel.

After any search: After any search: Contact Liberty (libertyhumanrights.org.uk) or your local legal aid solicitor if you feel your rights were not respected. You can also make a complaint to the Independent Office for Police Conduct (IOPC).

This guide may be freely shared, printed, and translated.

If you need help, call Migrant Help free, 24 hours a day, 7 days a week:

0808 8010 503