Digital Democracy Initiative

PEACE AND JUSTICE NETWORK
پیس اینڈ جسٹس نیٹ ورک پاکستان

CIVICUS

DIGITAL SAFETY TOOLKIT FOR HUMAN RIGHTS DEFENDERS

Safeguarding Freedom of Expression and Protecting Digital Defenders in Pakistan

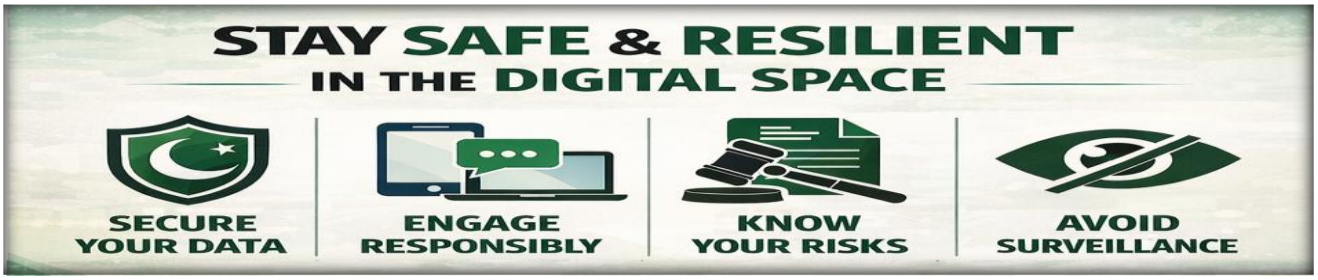
The Digital Safety Toolkit, developed by Peace & Justice Network Pakistan (PJN), empowers Human Rights Defenders (HRDs), civil society organizations, grassroots activists, lawyers, journalists, and community leaders to navigate the digital space safely, confidently, and effectively. It provides essential guidance for women's rights groups, minority rights organizations, defenders of fundamental freedoms, and advocates for transgender people, refugees, persons with disabilities, and children, ensuring that those working for justice and human rights can protect themselves, amplify their voices, and engage online without fear. Available in English and Urdu, it aims to ensure accessibility for diverse users working across Pakistan's civic and human rights landscape.

The Digital Safety Toolkit is structured into two key sections:

1. Digital Safety Tips for Human Rights Defenders in Pakistan
2. Work Safely in the Digital Space – Understanding the Prevention of Electronic Crimes Act (PECA)

These resources offer practical, step-by-step guidance on digital security, secure communication, responsible content creation, and effective online advocacy. They also provide clear, accessible explanations of the legal rights and protections available under international human rights frameworks, the Constitution of Pakistan, and national laws. Through real-life case studies, risk assessment tools, and structured incident response mechanisms, the toolkit equips defenders with actionable strategies to prevent and respond to online harassment, digital surveillance, misinformation, and cyber threats.

By strengthening digital resilience and building in-house expertise, the toolkit reduces dependence on external technical support and empowers defenders to sustain their advocacy even in high-risk or shrinking civic spaces. Peace & Justice Network Pakistan envisions this toolkit as a practical companion, a resource that fosters a safer, more secure, and rights-based digital ecosystem, enabling civil society across the country to engage, protect, and amplify their work with confidence.



DO's & DON'Ts for Safety & Protection of HRDs in Digital Space

For Journalists, Lawyers, NGOs, Activists, & Civil Society Defenders in Pakistan

Across Pakistan, human rights defenders (HRDs) including journalists, lawyers, activists, NGOs, grassroots organizers, and community advocates increasingly rely on digital platforms for documentation, advocacy, communication, mobilization, and public engagement. As civic space becomes more contested and constrained, the digital sphere has emerged as both a vital space for democratic participation and a growing arena of risk.

HRDs now face a wide spectrum of digital threats such as online harassment, trolling, hacking, doxxing, misinformation campaigns, targeted surveillance, digital criminalization, and the misuse of cyber laws. These threats not only impact individual defenders but also undermine public trust, silence marginalized voices, limit community engagement, and weaken democratic discourse.

The purpose of this Do's & Don'ts guide is to strengthen the safety, protection, and resilience of HRDs while they work in the digital sphere as safe and protected HRDs are essential for a healthy, vibrant, and democratic society.

This Do's & Don'ts guide is designed for practical use and may be adapted by organizations, networks, coalitions, media houses, bar associations, universities, and community groups as part of broader efforts to address the shrinking civic space and promote safe, open, and participatory digital environments.

COMMON DIGITAL THREATS HRD FACE

HRDs in Pakistan face several digital risks:

Online Harassment & Trolling

Coordinated abuse campaigns aimed at discrediting activists.

Defamation Complaints

Allegations that online posts damaged someone's reputation.

Cybercrime FIRs

Cases filed under PECA sections alleging:
Fake news
Hate speech
Cyber harassment
Unauthorized data access

Surveillance

Monitoring of social media activity or communications.

Device Seizure

Phones and laptops confiscated during investigations.

Doxxing

Publishing private information to intimidate.

Digital Safety Basics

Digital safety does not require advanced technical knowledge.
Some few basic steps can ensure your safety online

1. Personal Digital Security

Human rights work often involves sensitive information, field contacts, or documentation. If your personal devices or accounts are compromised, it can put you, your colleagues, or the communities you serve at real risk. Protecting your devices is the first barrier of defense.

☑ DO

- Use strong, unique passwords
- Enable Two-Factor Authentication (2FA)
- Update phones, laptops, and apps regularly
- Lock devices with PIN/password
- Backup important files offline & in secure cloud

✕ DON'T

- Reuse passwords
- Leave devices unlocked or unattended
- Store passwords in notes or messages
- Ignore system updates

2. Secure Communication

HRDs routinely share sensitive testimonies, evidence, cases, or political information. Communication channels that are insecure can expose sources, survivors, legal strategies, or advocacy plans to interception or misuse.

☑ DO

- Use encrypted apps like Signal or WhatsApp
- Verify identities before sharing info
- Use secure email providers for sensitive matters

✕ DON'T

- Discuss sensitive issues via SMS or open calls
- Forward confidential messages without consent
- Share files without encryption/password protection

3. Handling Sensitive Information & Evidence

Photos, documents, or testimonies collected by defenders can contain identifying details of victims or political actors. Losing control of this information can cause harm, retaliation, or legal threats.

☑ DO

- Encrypt confidential documents
- Anonymize reports (initials, age, area instead of names)
- Store evidence in multiple secure places

✕ DON'T

- Share identifiable data without consent
- Store evidence only on one device
- Publish photos with visible faces or GPS data

4. Social Media & Public Posting

Social media is a major advocacy space for HRDs in Pakistan. But careless posting can expose defenders, communities, or legal vulnerabilities. Thinking before posting can prevent unintended harm.

☑ DO

- Assess risks before posting
- Adjust privacy settings
- Use content warnings for sensitive content

✕ DON'T

- Reveal real-time locations or meeting spots
- Engage with trolls or coordinated harassment
- Share content exposing vulnerable groups

5. Working Under Surveillance Risk

Digital surveillance whether state, private, or political is becoming more widespread. HRDs should assume they may be monitored and take basic precautions to reduce tracking and interception.

☑ DO

- Use VPNs on public Wi-Fi
- Turn off unnecessary location tracking
- Limit microphone/camera permissions

✕ DON'T

- Connect to unknown/open Wi-Fi without VPN
- Leave apps with unnecessary permissions enabled
- Download unknown attachments or click suspicious links

6. Legal Literacy & Risk Awareness

Many digital activities fall under Pakistan's cyber and defamation laws. HRDs benefit from knowing what is legally protected and what could potentially be used against them in shrinking civic environments.

☑ DO

- Learn basics of PECA & defamation laws
- Consult lawyers for sensitive publications
- Save evidence of threats for legal action

✕ DON'T

- Assume everything online is legal speech
- Share unverified allegations about individuals
- Ignore digital threats or legal notices

7. Protecting Vulnerable Communities

HRDs often document abuses against women, children, minorities, refugees, laborers, and other vulnerable groups. Their digital exposure can lead to retaliation, stigma, surveillance, or violence. Consent and confidentiality matter.

☑ DO	✕ DON'T
• Get informed consent before documenting • Blur faces & remove identifiers • Understand gendered and minority-specific risks	• Expose survivors' identities • Share data that links to homes, workplaces, or villages • Publish content without community approval

8. Mental Health & Psychosocial Safety

HRDs and journalists face burnout, threats, online harassment, trolling, smear campaigns and trauma from digital work. Protecting mental well-being helps defenders sustain their activism long-term.

☑ DO	✕ DON'T
• Take regular digital breaks • Seek peer support networks • Report harassment to trusted allies	• Internalize harassment or blame yourself • Work nonstop without boundaries • Ignore signs of anxiety, stress, or trauma

9. Organizational Preparedness

Digital safety is not only an individual responsibility. Organizations play a crucial role by creating systems, protocols, and training that protect their staff, volunteers, sources, and communities.

☑ DO	✕ DON'T
• Develop digital safety policies • Train staff on digital emergencies • Assign digital safety focal points	• Depend entirely on informal practices • Assume everyone has the same risk exposure • Leave sensitive data unprotected across teams

10. Dealing with Harassment, Threats & Attacks

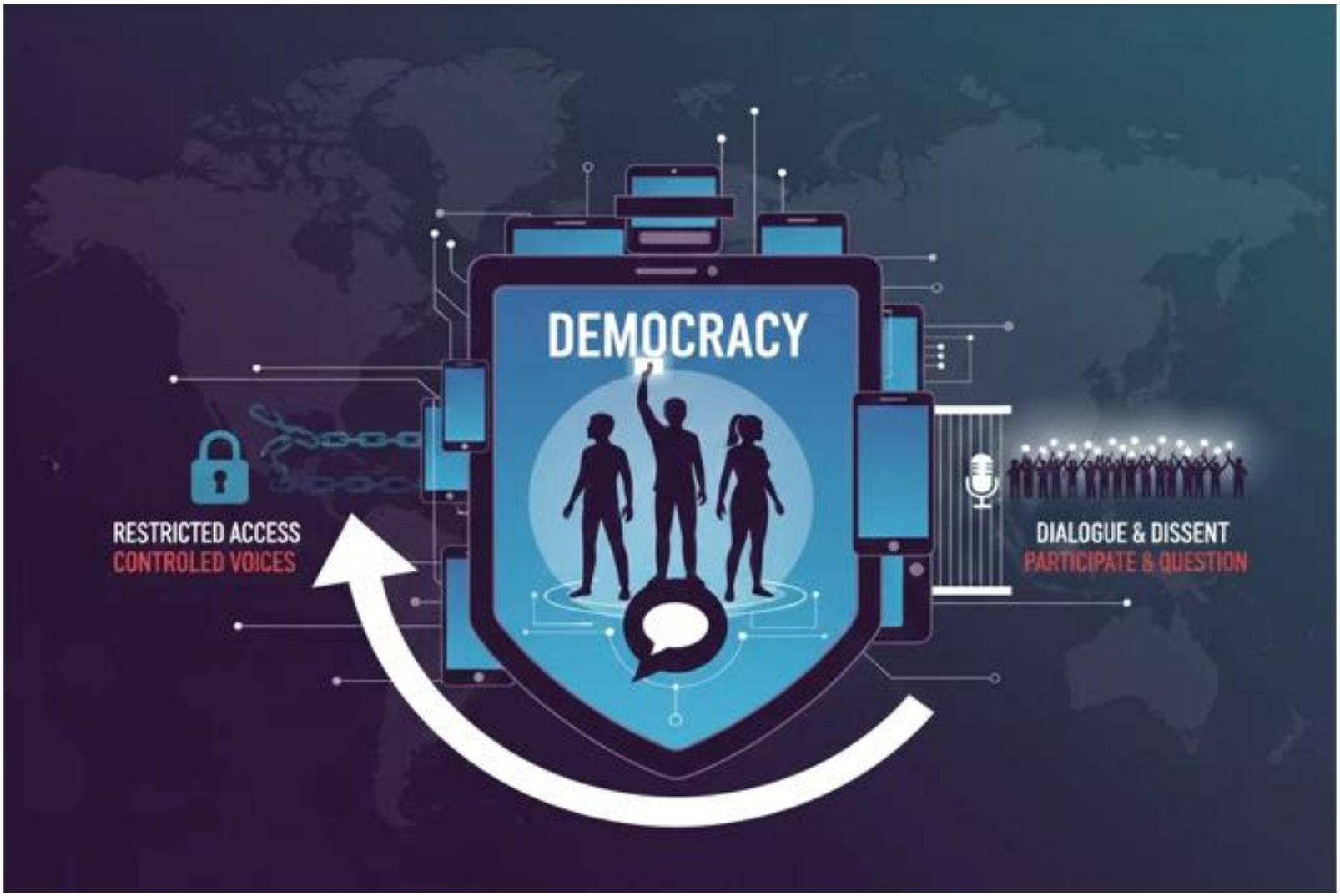
Online attacks against HRDs including trolling, doxxing, hacking, impersonation, and smear campaigns are increasing in Pakistan. Responding strategically rather than emotionally helps reduce harm.

☑ DO

- Document incidents (screenshots, URLs, timestamps)
- Report to platforms & support networks
- Alert your colleagues for awareness

✕ DON'T

- Respond to harassers directly
- Delete evidence without saving
- Downplay or ignore coordinated attacks



Digital Safety and Protection

Protecting Rights, Securing Digital Space

Legal Awareness	Digital Threats	Device & Account Security	Secure Communication
Know key laws - PECA, PPC, privacy rights.	Recognize monitoring, harassment, malware.	Use strong passwords, 2FA, encryption.	Encrypted chats, VPN use.

Social Media Safety	Online Harassment	Phishing & Malware	Data Protection
Privacy settings, limit sharing location.	Document threats, report abuse.	Avoid suspicious links & emaiis.	Encrypted storage, secure backups.

Human Rights Lawyers	Journalists	Rights Defenders	Mental Wellbeing
Secure client data, case files.	Protect sources, remove metadata.	Safeguard community information.	Take breaks, seek support.

Incident Response	Organizational Safety
Report breaches, change passwords.	Training & protocols for staff.

Additional Threats and Safety Tips for Human Rights Defenders in Pakistan

Stay Safe, Stay Protected

Spyware & Keyloggers

Example: HRD unknowingly installs a dubious app that records keystrokes.

- Use verified apps only from trusted sources.
- Install antivirus & spyware scanning software
- Scan attachments & downloads before opening

Ransomware

Example: HRD opens malicious file; system locked and ransom demanded.

- Regularly back up important files.
- Avoid downloading unknown email attachments or links from untrusted sour
- Keep AV & OS updated to close ransomware avenues.

Stalking & Location Tracking

Example: HRD posts event photos; attackers identify their location.

- Disable geotagging on-photos & avoid real-time location sharing.
- Use a VPN to mask and protect online activity
- Keep AV & OS updated to close ransomware avenues.

Credential Theft & Spear Phishing

Example: Attackers send HRD a personalized email pretending to be org head.

- Verify sender's authenticity before clicking links or responding.
- Do not share passwords via risky channels like email.
- Use a password manager to generate and store unique passwords.

Account Hijacking

Example: HRD's social media account is taken over, posts made impersonating them.

- Use Strong, Unique Passwords & Two-Factor Authentication (2FA)
- Be Wary of Phishing & Suspicious Links
- Regularly Monitor Accounts & Update Devices

Content Tampering & Fake Evidence

Example: Manipulated images/videos fabely atributed to HRD..."

- Keep original digital files backed up in a ssoure location.
- Check media for edits or unusual metadata.

Additional Threats and Safety Tips for Human Rights Defenders in Pakistan

Stay Safe, Stay Protected

Surveillance & Monitoring

Example: Authorities track rights defender's emails, calls, and movements.

- Use encrypted chat apps like Signal
- Turn off location services/avoid real-time sharing.
- Use VPN to mask online activities.

Online Harassment

Example: Fake profiles defame and threaten HRD posting about women's rights.

- Document threatening messages & posts.
- Report & block harassers on social media,
- Adjust privacy settings to limit comments/ shares.

Phishing & Spear-Phishing

Example: HRD receives email saying account compromised, asked to reset password.

- Verify sender's email before clicking links.
- Hover over links to see actual URL destination.
- Do not enter passwords/personal info in emails.

Malware & Hacking

Example: HRD opens document that installs keylogger, records keystrokes.

- Install antivirus, enable automatic updates for devices.
- Scan attachments with antivirus before opening.
- Use long, unique passwords with two-factor authentication.

Fake News & Disinformation

Example: False posts claim HRD is anti-state, stirring hate online.

- Report falke information to social media platforms.
- Issue factual clarifications via secure channels if safe.
- Seek help from digital rights groups to counter misinformation.

Doxxing & Data Breaches

Example: Home address, phone number of HRD leaked online.

- Limit sharing personal data publicly.
- Secure sensitive files with encryption & strong passwords.
- Have a plan to alert targeted family/friends.

Best Practices for Secure Messaging

Verify Contacts

Ensure you are communicating with the correct person. Signal allows verification of contact keys to prevent impersonation

Use Disappearing Messages

Enable automatic deletion of messages after a set period. This minimizes risk if a device is lost or seized.

Limit Screenshots and Forwarding

Sensitive information should not be captured via screenshots or forwarded outside trusted networks.

Separate Personal and Work Accounts

Maintain a dedicated account for advocacy or HRD work to prevent accidental exposure.

Combine Messaging Security with Device Security

Even encrypted apps cannot fully protect communications if your device is compromised. Combine encrypted messaging with:

- Strong device passwords or PINs
- Two-factor authentication
- Regular software updates
- Encrypted device storage

When combined with strong device security and responsible messaging practices, it allows you to communicate freely while protecting yourself, your team, and the people whose stories you are documenting.

Reporting & Responding to Digital Threats

Document Everything Immediately

Before reporting or responding publicly, preserve evidence. Capture:

- Screenshots of messages, profiles, comments, and posts
- Full URLs of offending content
- Usernames and profile links
- Dates and times (including your time zone)
- Any prior interaction history

Secure Your Accounts

Before filing a complaint:

- Change your passwords immediately.
- Enable two-factor authentication (2FA).
- Review account recovery emails and phone numbers.
- Check for unknown login sessions.
- Inform trusted contacts not to click suspicious links sent from your account.
- If your account has been hacked, report it to the platform immediately.

Report to Authorities

In Pakistan, cybercrime complaints can be filed with the:

National Cyber Crime Investigation Agency

Sending an email to:
helpdesk@nccia.gov.pk

24/7 Helpline:1799

Online Complaint Portal:
https://complaint.nccia.gov.pk

Ministry of Human Rights Helpline 1099

You may:

- File an online complaint through the portal
- Visit the nearest NCCIA Cyber Crime office in person
- Call their helpline

Use Platform Reporting Mechanisms

In addition to filing with authorities:

- Report abusive accounts directly to the platform (Facebook, X, Instagram, etc.).
- Request removal of harmful content.
- Save confirmation emails of your reports.
- Platform reports create a documented trail of abuse.

Inform Trusted Networks

- If harassment is targeted and coordinated:
- Inform your organisation or HRD network like HRCP, Freedom Network, Digital Rights Foundation or PJN Digital Defender Portal.
- Alert digital rights organisations.
- Consider a collective response if safe.
- Public exposure of coordinated harassment sometimes discourages attackers — but this should be done carefully and strategically.

REMEMBER!

When responding to digital threats:

- ✓ Document first
- ✓ Secure your accounts
- ✓ Report strategically
- ✓ Seek legal advice if necessary
- ✓ Preserve evidence safely
- ✓ Protect your emotional well-being

PEACE AND
JUSTICE NETWORK
پیس اینڈ جسٹس نیٹ ورک پاکستان

CONSTITUTION OF PAKISTAN ARTICLE 25 (1)

EQUALITY OF CITIZENS

All citizens are equal before law and
are entitled to equal protection of law.

CONSTITUTION OF PAKISTAN ARTICLE 19

FREEDOM OF SPEECH & EXPRESSION

Every citizen shall have the right to
freedom of speech and expression.

DIGITAL RIGHTS ARE HUMAN RIGHTS

Every citizen in Pakistan has the right to privacy,
protection, safety, and freedom of expression.

PEACE & JUSTICE NETWORK

/PJNPakistan /PJNPakistan /PJNPakistanofficial www.pjn.org.pk contact@pjn.org.pk