

Promoting a Safer Environment for **Women in the Media**

A Resource Kit

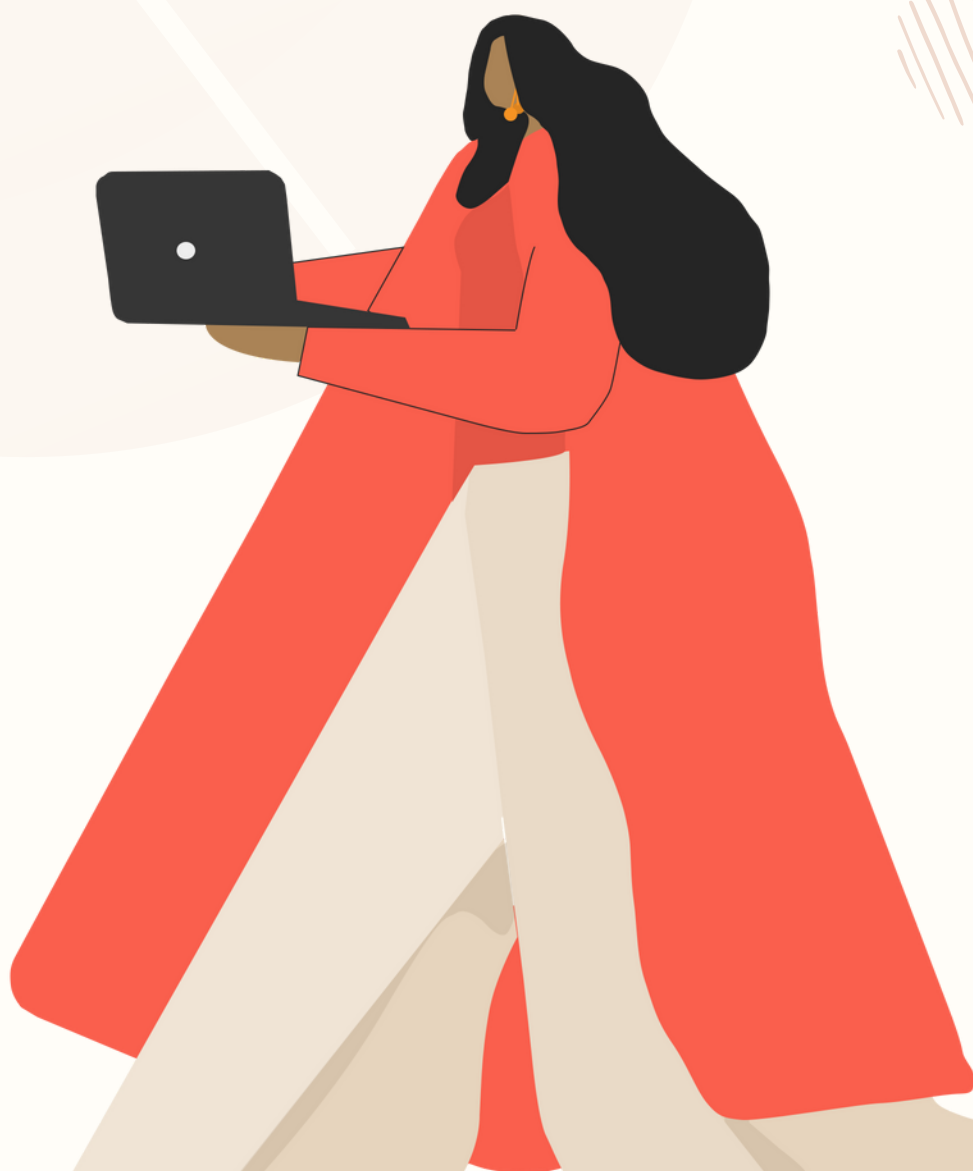


Table of Contents

00 — Note

01 — Digital Safety

1.1 — Safety Basics

1.2 — Level Up

1.3 — Self-help Guides

1.4 — Digital Checklist

02 — Editorial Guidelines

2.1 — Editorial Guidelines: Dos and Don'ts

03 — Laws

3.1 — Laws: Help or Harm

3.2 — Reporting Protocols

3.3 — Seeking Help

3.3 — Legal Checklist

04 — Understanding Key Concepts Through Videos

4.1 — Mental Health by Dr. Asha Bedar, clinical psychologist

4.2 — How to report unlawful activity, abuse, and threats by Hyra Basit, Helpline Manager, Digital Rights Foundation

4.3 — Reporting under the law by Imaan Hazir-Mazari, lawyer

4.4 — Trolling is a tool of gendered disinformation, Nina Jankowicz, researcher and writer

Annex — Digital Risk Assessment Form

Note

Nearly two-thirds of the women journalists from 125 countries surveyed for the United Nations Educational, Scientific and Cultural Organization's (UNESCO) 2021 report *The Chilling* said they had suffered from varying degrees of online violence. A small fraction received support from their media organizations while only 11% went to the police. The impact on freedom of speech and the toll on mental health is incalculable and too often underestimated.

This Digital Safety resource kit has been designed to serve as a one-stop resource for how to protect, prevent and seek help when using digital devices or while engaging on social media. From basic safety, to platform guidelines, relevant laws that help or could harm journalists, reporting protocols for legal remedies to editorial guidelines, the kit has been created based on the experiences of experts and journalists.

CEJ-IBA would like to thank Farieha Aziz, the Legal Aid Society (LAS), Shaheryar Popalzai, and Imaan Mazari-Hazir, the Digital Rights Foundation's Zoya Dawar, and Dr. Asha Bedar for their invaluable contributions to this resource kit. Most of all, the CEJ-IBA is grateful for the generous support of UNESCO for funding a resource tailored to the specific needs of Pakistani journalists.

Authors:

Farieha Aziz
Amber Rahim Shamsi

Coordinator:

Syeda Fizza Abid

Design:

Farwah Rizvi

Videos:

Eman Lakhani

Digital Safety



1.1 Safety Basics

Passwords

- Use a **different** password for every account
- **Avoid** using passwords associated with you or people you know
- Use a **secure password manager** to generate and store passwords securely
- Make sure your devices are **protected** by a password or pincode
- Change the **generic password** provided on your wi-fi device
- Keep your passwords **private** – never share a password with anyone else
- Do not write down your passwords
- Use passwords of at least eight (8) characters or more (longer is better)
- Use a **combination** of uppercase letters, lowercase letters, numbers, and special characters (for example: !, @, &, %, +) in all passwords
- **Avoid** using people's or pet's names, or words found in the dictionary; it's also best to avoid using key dates (birthdays, anniversaries, etc.)
- Substituting look-alike characters for letters or numbers is no longer **sufficient** (for example, "Password" and "P@ssw0rd")
- A strong password should look like a series of **random characters**

STEPS TO CREATE A STRONG PASSWORD

Think of a phrase or sentence with at least eight words. It should be something easy for you to remember but hard for someone who knows you to guess. It could be a line from a favorite poem, story, movie, song lyric, or quotation you like

I Want To Put A Dent In The Universe

Remove all but the first letter of each word in your phrase

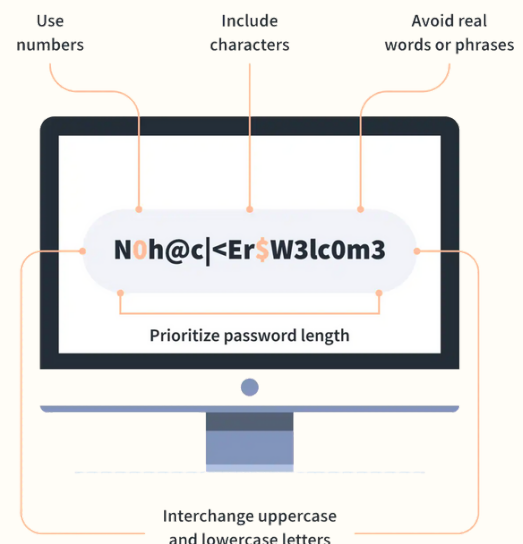
IWTPADITU

Replace several of the upper-case letters with lowercase ones, at random. Now substitute a number for at least one of the letters

iWtpAD1tU

Finally, use special characters (\$, &, +, !, @) to replace a letter or two -- preferably a letter that is repeated in the phrase. You can also add an extra character to the mix.

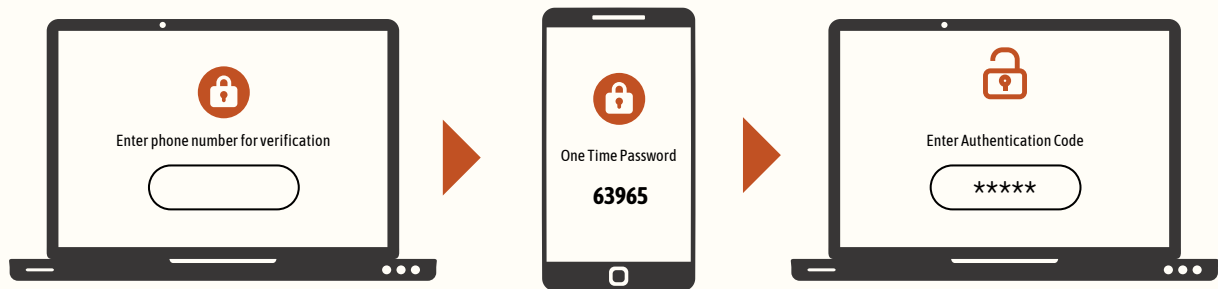
iW+pAD1tU!



Two-Factor Authentication

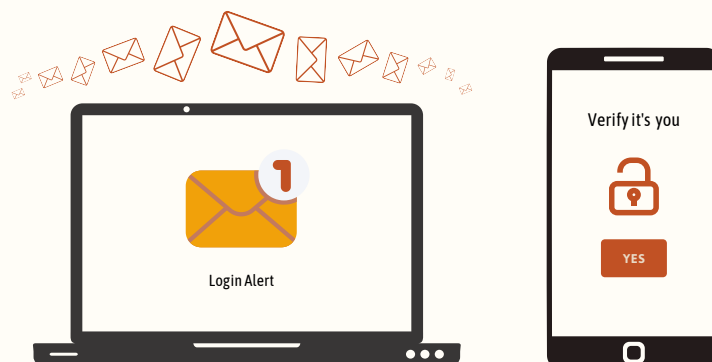
- **Activate** two-factor authentication for every platform that offers it
- Download **backup codes** in case you do not receive the code

Example of Two Factor Authentication



Login Verifications

- **Activate** login verifications for every platform that offers it to be alerted each time your account is logged into
- Check where you are logged in from
- If you do not recognize a device or activity, end the session and change your password immediately



Get Verification Alerts through Email or Phone

Recovery Information

- Add a recovery email address and phone number - ones you have access to; in case your account is ever compromised, this will enable you to recover it and regain access

Browsers

- Use **incognito** mode
- Erase browser history
- Allow only essential cookies
- Activate the Do Not Track setting in your browser settings
- Use a browser that allows you to add extensions and add-ons for increased privacy and safety
- Ensure your connection is **secure** by clicking on the lock in the top left corner to check for HTTPS

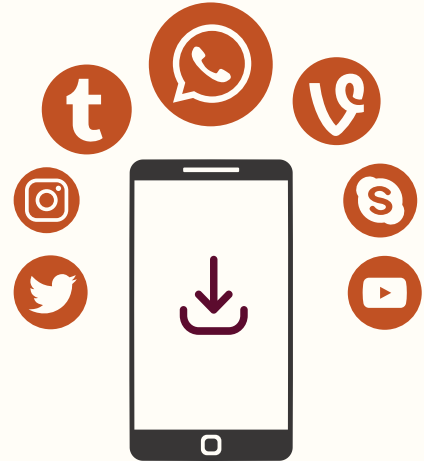


Devices

- Regularly **scan your device** by using an anti-virus software
- Encrypt your hard drive
- Backup data to the cloud and an external hard drive
- Activate 'find my phone' or 'find my device' settings for **tracking and recovery** of a lost/stolen device
- Know your phone's IMEI number to have the handset blocked if unrecoverable once stolen or lost
- Wipe your phone's screen regularly to **remove smudge marks** that may indicate your pin
- iOS devices keep a record of all your location data, keep location off
- Reload OS on device if you suspect malware
- Use a strong credential to protect your mobile device
- Turn off Bluetooth, Wi-Fi, and location when not using it
- **Backup your mobile device**; note if you use Google authenticator you cannot transfer 2FA codes to a new phone

Apps

- Only download applications from **trusted sources** (i.e. Google Playstore, Apple Store)
- Be aware of the permissions you grant to apps you download
- Keep your mobile OS and apps updated
- Delete apps that are obsolete and no longer have support
- Install Brave browser (privacy-based), NYC Secure (mobile IDS), Signal or Wickr (secure messengers)



Social Media Platforms

- Provide only what is necessary on the backend
- Be aware of what information you post
- Never share home addresses
- Avoid providing location information
- Be mindful of the identity information you share especially something that can put minors at risk
- Frequently revisit **privacy settings** as they tend to change
- Familiarize yourself with reporting mechanisms



Never



- Share or save your passwords or banking information in auto-fill forms or Remember Me settings
- Click on random links
- Accept media or download files from unknown sources and people
- Leave auto download on
- Auto-join unfamiliar networks
- Download apps from a browser
- Grant administrator access to anyone, even in the workplace; if you need to, make sure you're monitoring everything
- Trust messages that ask for **ANY** kind of personal information
- Post medical history, credit or debit card information, wage or salary information, CNIC number, Personal address, bank, and financial information, driver's license, any other government-issued ID, passport number

Remember

- Anything you put up online or on a device connected to the Internet leaves a **digital footprint**
- Information you share is stored on the servers of your Internet service provider and platform
- A digital trace leads back to you and you bear legal liability for activity through devices and connections registered in your name
- Keep your Wi-Fi off if you're not using it
- Always make sure you're on a secure Wi-Fi before sending sensitive information
- Despite erasing, data is recoverable
- Factory reset the device, overwrite, and reset again if you are passing it on to someone else or selling it
- Always check a website's legitimacy using Netcraft or PhishTank



1.2 Level Up

The right settings and practices can provide a great degree of protection on a day-to-day basis, but there are always vulnerabilities, especially due to human error and judgment. It is important to understand the manner in which you can be targeted, how such attempts work, and what to do.

Social Engineering

Avast defines social engineering as “using psychological techniques to manipulate behavior” by “encouraging victims to act against their interests.” In terms of information security, this would mean getting people to give their private data such as login details or financial information online.¹

Social engineering deceptively manipulates people into performing actions or divulging login information or confidential information.

Social engineering can be performed in person, using a paper-based delivery method (like the postal service), over a phone, or digitally/online.

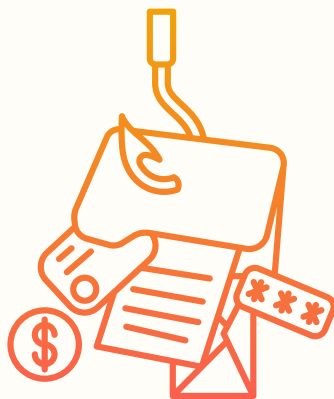
Types of social engineering



¹ <https://www.avast.com/c-social-engineering>

Phishing

The Center for Democracy and Technology explains phishing as: “The most common vector for cybercrime is phishing, where an attacker attempts to trick a user into taking a certain action in response to an email or other message like clicking on a link, downloading a file, or revealing personal or confidential information. The access gained by the attacker can provide them with a way to download malicious software onto the user’s system, allowing them to steal data or damage the system.”²



Email
Spear
Whaling
Smishing and
vishing
Angler

Digital Attacks

Phishing	Spear Phishing	YOUR role
Email-based social engineering targeting an organization	Email-based social engineering targeting a specific person or role	STOP, LOOK, and THINK before clicking on a link or opening an attachment

Mobile/Phone attacks

Smishing	Vishing	YOUR role
Text-based social engineering	Over-the-phone-based social engineering	STOP, LOOK, and THINK before clicking on a link in a text message or divulging sensitive information over the phone ²

² <https://cdt.org/insights/prevention-and-mitigation-of-successful-phishing-attacks/>

Email red flags - FROM

- I don't recognize the sender's email address
- This email is from someone outside my organization
- This email was sent from someone I know and is very unusual or out of character
- Is the sender's email address from a suspicious domain (like micorsoft-support.com)?
- I don't know the sender personally
- I don't have a relationship nor any past communication with the sender
- This is an unexpected or unusual email with an embedded hyperlink or an attachment

Email red flags - TO

- I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to
- I received an email that was also sent to an unusual mix of people

EXAMPLE: It might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses

Email red flags - SUBJECT

- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

Email red flags - DATE and TIME

- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?



Email red flags - HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the link-to address is for a different website (This is a big red flag)
- I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank
- I received an email with a hyperlink that is a misspelling of a known website. For instance, www.dawnnews.com — this isn't a legit domain

Email red flags - ATTACHMENTS

- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message
- I see an attachment with a possibly dangerous file type
- The only file type that is always safe to click on is a .txt file

Email red flags - CONTENT

- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click on a link or open up an attachment that seems odd?
- Do I have an uncomfortable feeling about the sender's request to open an attachment or click on a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

General email subjects

- Password Check required immediately
- Touch base on meeting next week
- Important: Dress Code Changes
- Scheduled Server Maintenance
- Deactivation of [email] in Process
- Please review
- You have been added to a team/channel on [messaging platform]

Emails from social media linked accounts

LinkedIn

- You appeared in new searches this week
- People are looking at your LinkedIn page
- Please add me to your LinkedIn network
- LinkedIn Password reset
- Join my network on LinkedIn



Twitter

- Someone has sent you a direct message on Twitter

Facebook

- New Sign-in to your Facebook from Samsung Galaxy S4
- You were tagged in 3 photos on Facebook



1.3 Self-help Guides

Support Centres and Reporting to Platforms

All email service providers and social media platforms have support or help centers, to understand settings and troubleshoot problems. Content-sharing platforms and social media platforms are governed by their own rules and community guidelines, each distinct from the other. Whichever service you use, ensure you are aware of both the settings you should activate and the rules that govern the content on these platforms.

Platforms



Google Account



Google safety center



Facebook



Messenger



Instagram



Whatsapp



Tiktok



YouTube



Twitter



Zoom

Device Safety



Apple/iOS



Samsung

Other Guides



CPJ



Tactical Tech



UNESCO



UNESCO MOOC on 'How to report safely: Strategies for women journalists and their allies'



PEN America



Council of Europe



Centre for Law and Democracy



Troll Busters

1.4 Digital Checklist



Do you have a different password for every account?



Do you have password/pin/fingerprint protection on your phone?



Is your laptop protected with a password?



Is your laptop encrypted?



Do you have two-step verification for all the services that offer it?



Do you have login verifications for all services that offer it?



Do your accounts have backup email addresses and phone numbers listed for recovery?



Editorial Guidelines



2.1 Editorial Guidelines: Dos and Don'ts

Don't Be Stupid

General Tips

- Resist falling into the informality trap of social media, which makes it easy for the lines between professional and personal to be blurred
- Remember the difference between what needs to be public and what needs to be private
- Value both your account and your profession
- You don't need to comment on everything – some news and views can be private
- Be careful about how much you want to reveal – information published on the web is almost impossible to remove

Personal Use

Dos

Balance - Anyone can see the individuals, issues, or organizations that you choose to friend or follow on social media

- ✓ Do consider the impression given by these choices, especially if they are contentious or partisan, and *relevant* to the stories you cover
- ✓ Do broaden or balance the range of social media posts that you publicly favorite, save, like, or retweet

Retweets are seen as endorsements – A 'retweets aren't endorsements' disclaimer won't be enough, especially if it is without context, and you and your work will be associated with anything you retweet or repost

- ✓ Do provide context to your RTs, through a running thread, or by sharing diverse sources of RTs on the same issue

Second pair of eyes – Social media platforms are not our personal journals and there can be consequences of our mistakes in terms of credibility or legal liability

- ✓ Do show your post to a colleague or friend before posting whenever possible, unless under exceptional circumstances
- ✓ Do be transparent and admit when you're wrong online

Security – Just as we lock our homes before we leave the house, it is as important to keep our social media accounts safe. Online harm is as damaging as real-world harm, especially given the quantity of personal information stored on our social media accounts

- ✓ Do ensure two-step verification for every social media account you manage
- ✓ Do use secure passwords, change them often, and don't store or send them via email

Don'ts

Avoid posting content that could:

- ✗ Provoke, attack or offend others
- ✗ Breaks or condones breaking the law
- ✗ Contains language that may offend, including swear words
- ✗ Be racist, sexist, homophobic, sexually explicit, abusive, or otherwise unacceptable
- ✗ Be from a person who is impersonating somebody else



Professional Use

Emergencies/Big events/Breaking news

- Remember – it is better to be right than first
 - The subject of your post is a human being too
 - Give clear warnings about sensitive content
 - Ensure next of kin do not hear about death or injuries via your social media
 - UGC (User Generated Content) – Video and stills on the web aren't 'in the public domain' and free for us to use
- At least 3 pairs of eyes should review UGC before posting
 - Permission should be sought before posting or credit must be given when posting UGC – bear in mind that the copyright holder probably won't be the person shown in the content and may not be the person who took it, or distributed it
 - Giving the name of the website or platform may not be enough for credit, effort should be made to give on-screen credit to the individual who owns the content, unless they ask for privacy due to the potential for risk or harm
 - Potential contributors may feel vulnerable or distressed so it is best to move conversations about permissions to private channels such as direct or indirect messaging or email
 - Public requests to use content may also give credence to rumors or hoaxes
 - We must also never ask potential contributors/non-professional individuals at the site of news events to take risks for our content



Laws



3.1 Laws: Help or Harm

Laws can be both helpful and harmful. Some laws provide remedies whereas others are used to silence individuals, especially journalists. The table below distinguishes between the two, based on how the laws have been applied in Pakistan.

Law	Help	Harm
Journalist Safety	The Sindh Protection of Journalists and other Media Practitioners Act, 2021 Protection of Journalists and other Media Professionals Act, 2021	
Harassment	Protection Against Harassment of Women at the Workplace (Amendment) Act, 2022 Section 509 of the Pakistan Penal Code	
Assault	Section 354 of the Pakistan Penal Code	
Criminal Intimidation	Section 506 of the Pakistan Penal Code	
Cybercrime	Sections 21 and 24 of The Prevention of Electronic Crimes Act (PECA), 2016	Sections 10, 11, 20 and 37 of The Prevention of Electronic Crimes Act (PECA), 2016
Defamation		Sections 499 & 500 of the Pakistan Penal Code Defamation Ordinance 2002
Sedition		Section 124-A of the Pakistan Penal Code

Law	Help	Harm
Promoting enmity		Section 153-A of the Pakistan Penal Code
Terrorism		Section 6 of the Anti-Terrorism Act, 1997
Public mischief		Section 505 of the Pakistan Penal Code
Abetment of insubordination or mutiny		Sections 131 and 138 of the Pakistan Penal Code
Contempt of court		Section 5 of the Contempt of Court Ordinance 2003
Right to Information Laws	<p>The Khyber Pakhtunkhwa Right to Information Act 2013</p> <p>The Punjab Transparency and RTI Act 2013</p> <p>Sindh T&RTI Act 2016</p> <p>Right of Access to Information Act 2017 (Federal)</p> <p>The Balochistan Right to Information Act, 2021</p>	
Justice of Peace	22-A & B of the Code of Criminal Procedure	
Habeas Corpus	Article 199 of the Constitution of Pakistan	

Journalist Safety

The aim of both laws is to “promote, protect and effectively ensure the independence, impartiality, safety, and freedom of expression” of journalists and media professionals/practitioners.

THE SINDH PROTECTION OF JOURNALISTS AND OTHER MEDIA PRACTITIONERS ACT, 2021

It places an obligation on the provincial government to ensure the protection of right to life, safety and security of journalists and media practitioners. It requires the government to take necessary steps against harassment, violence and threats of violence, and protects against the disclosure of professional sources of information.

The law establishes the Commission for the Protection of Journalist and other Media Practitioners (CPJMP), which will probe complaints of harassment, sexual harassment, violence and threats of violence.

It places an obligation on employers to provide adequate insurance and training to their employees, who are at risk of being attacked, injured or killed due to their work.

PROTECTION OF JOURNALISTS AND OTHER MEDIA PROFESSIONALS ACT, 2021

With jurisdiction limited to the federal capital, the objectives of the law are to ensure journalists and media professionals have the right to life and protection against ill-treatment; the right to privacy and non-disclosure of sources; protection from abusive, violent, and intolerant behavior; protection against harassment.

Under the Act, a Commission for the Protection of Journalists and Media Professionals is to be established, the commission is under obligation to investigate, prosecute and penalize threats, coercion, acts of violence and abuse of journalists and media professionals.

Details of the journalist welfare scheme are provided in Schedule 1, which outlines the duties and obligations of employers, including the provision of necessary life and health insurance.



Harassment

PROTECTION AGAINST HARASSMENT OF WOMEN AT THE WORKPLACE (AMENDMENT) ACT, 2022

Explanation: The definition of sexual harassment has been expanded so that it is not limited to acts explicitly sexual in nature.

The definition now includes “discrimination on the basis of gender, which may or may not be sexual in nature.”

Harassment can be physical, verbal, non-verbal, gestures, through digital means, sexual or derogatory attitudes, or actions that interfere with work or create a hostile environment.

Comment: Originally enacted in 2010, over the years it became apparent there was a need to expand the law to include a wider range of professionals who qualify as complainants - including students - which led to the 2022 amendments.

Process: All organizations are mandated to set up a three-member committee to inquire into complaints; at least one member of the committee must be a woman.

Where such a committee does not exist, a complaint can be filed with the ombudsperson.

Punishment: Both the committees and ombudspersons are empowered to award certain penalties laid out in the 2010 law. Appeals lie to the governor (in provinces), the President, and then the High Court and Supreme Court.

SECTION 509 OF THE PAKISTAN PENAL CODE (PPC)

Insulting the modesty or causing sexual harassment is a criminal offence under the PPC, a complaint for which must be filed at a local thana (police station). This too covers words, gestures, and acts, whether in a public space or a workplace. Section 509 is a punishable offence with imprisonment up to three years or with a fine up to five hundred thousand rupees.

Assault

Section 354 (Assault or criminal force to woman with intent to outrage her modesty)

Explanation: Use of criminal force to harm a woman's modesty or assault with the intent of outraging modesty.

Criminal force is when a person intentionally uses force on another person without that person's consent, with the prior intention of causing harm to that person in the form of injury, fear, or annoyance to whom the force is used.

Assault is a gesture made to any person, knowing that it will be apprehended to use criminal force, such as shaking a fist at someone with the intention to strike

Harming modesty could include making physical sexual overtures

Punishment: 2 years imprisonment or a fine; or both.

Criminal Intimidation

Section 506 (Punishment for Criminal Intimidation) underscores that anyone who commits criminal intimidation will be subject to a punishment of either jail for up to two years, a fine, or a combination of the two. If there is a threat to bring about death or great harm, or destruction of property, or to bring about an offense that is punishable by death or life in prison will be punished by imprisonment of either description for a term that may last up to seven years, or by fine, or by both.

Cybercrime

THE PREVENTION OF ELECTRONIC CRIMES ACT (PECA), 2016

Section 10

Explanation: Covering the offence of cyber terrorism, an act or threat towards the government, public or community; the advance of interfaith, sectarian or ethnic hatred; and supporting the objectives of proscribed organizations. This is a cognizable offence, an FIR can be registered and person arrested.

Punishment: Up to 14 years imprisonment and upto Rs. 50 million fine

Section 11

Explanation: The spread of hate speech by advancing interfaith, sectarian or racial hatred through electronic means.

Punishment: Up to 7 years imprisonment, a fine or both.

Section 20

Explanation: Transmission and posting of any information which is false, intimidates or harms the reputation or privacy of a natural person

Punishment: Up to 3 years imprisonment and a fine of up to Rs. 1 million.

Comment: While these sections are meant to curtail crimes, the manner of their application is a source of concern. These sections have been used repeatedly against journalists to silence their critique of state actions and policies, or the conduct of state officials.



Though not applicable with respect to remarks about state institutions or officials, these sections have been wrongly added to FIRs against journalists.

Under criminal law, an accused must secure bail and show up at every hearing. How long a case runs on, there is no timeframe.

With respect to Section 20, the “harm to reputation” part of the law was struck down as unconstitutional by the Islamabad High Court in response to petitions filed by journalists challenging its application and language. However, a conflicting judgment of the Lahore High Court in a prominent actress/singer’s case, upheld Section 20 as constitutional prior to the IHC decision. The appeal against the LHC verdict is currently pending before the Supreme Court, which will deliver a final verdict on the law.

Section 20 has also been used by those accused of sexual harassment and misconduct, to silence disclosures made against them, as well as journalists who have reported on this topic.

Section 21

Explanation: Superimposing a picture or video of a person in sexually explicit manner and transmitting or exhibiting it publicly.

Punishment: 5 years imprisonment and a fine of up to Rs. 5 million or both.

Section 24

Explanation: Cyberstalking, such as following or contacting a person, monitoring their online activity; spying and causing harm or distress; taking a photograph making a video without consent causing harm with the intent to coerce, intimidate or harass a person.

Punishment: Up to 3 years imprisonment and a fine of up to Rs. 1 million or both.

Comment: For these offences, a complaint has to be filed with the FIA. Section 21 is a cognizable offence, which means the FIA can proceed with an FIR and make an arrest, whereas if the complaint falls under Section 24, they have to approach the court with an application for permission to investigate.

Section 37

Explanation: Though not a criminal offence, the section copy pastes Article 19 from the Constitution of Pakistan and gives PTA the authority to interpret and apply the exceptions listed.

It is under Section 37 that the contentious social media rules were notified, and content-blocking on the Internet is carried out, sometimes with complete shut-downs of websites and apps.

Content owners and social media platforms are also sent takedown notices by PTA to remove said content from their sites under Section 37.

Defamation

Comment: Both civil and criminal defamation laws have been used against journalists by the state and private individuals to silence them.

499 & 500 OF THE PPC

Explanation: If by words spoken or written, signs and visual representations, someone makes or publishes any imputation concerning another that intends to harm the reputation of a person is liable to the offence of defamation

Punishment: Up to 2 years imprisonment up to two years, a fine or both. The originator of such an offence can be punished with imprisonment of up to 5 years.

Comment: Ten exceptions to defamation are built into the law which primarily have to do with public good, public performance and conduct of public servants, good faith comment etc.

The problem is not whether there will be a conviction but what a charge involves, as it forces the accused to seek legal help - which can be exorbitant if not pro bono or at a reduced fee - and they are dragged through the process of showing up for hearings with no fixed timeframe for the conclusion of the case.

DEFAMATION ORDINANCE 2002

Explanation: Publication without proof is actionable under the defamation law.

Defamation is defined as any “wrongful act or publication or circulation of a false statement or representation made orally or in written or visual form which injures the reputation of a person, tends to lower him in the estimation of others or tends to reduce him to ridicule, unjust criticism, dislike, contempt or hatred shall be actionable as defamation.”

There are eight defenses built into the law.

Process: Under the Ordinance, the person who has been defamed first sends a notice to which the recipient can respond to. Following this, if a case is pursued, the trial is conducted in the district court.

Punishment: If defamation is proven, the court can instruct the defendant to issue an apology and/or pay compensatory damages.



Sedition

124-A OF THE PPC

Explanation: "Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Federal or Provincial Government established by law"

Punishment: 3 years to life imprisonment and/or a fine.

Comment: This section has been added in FIRs against journalists when they have critiqued state policies and the conduct of state officials.



Right to Information Laws

Right to Information laws have been adopted at the federal and provincial levels. These have been enacted under Article 19-A. Each of them lay out a process and timeframe within which requests must be complied with, failing which applicants may approach the relevant information commission against the non-provision of information.

KHYBER PAKHTUNKHWA RIGHT TO INFORMATION ACT 2013

Public body must respond within 10 days or receipt of request, which can be extended for a further 10 days.

A designated officer must facilitate these requests.

It is a criminal offence under this law to obstruct access to a record or destroy it, interfere with or obstruct the working of the Information Commission or public body duty bound by the law, use information malafidely for purposes other than expressed.



Right to Information Laws

Whistleblowers who out wrongdoing that constitutes a criminal offence, are protected under the law.

THE PUNJAB TRANSPARENCY AND RTI ACT 2013

Public bodies are required to proactively disclose information and designate public information officers.

Public body must respond within 14 days or receipt of request, which can be extended for a further 14 days.

If information is not provided, an applicant can file an internal review with the head of the public body or approach the information commission.

It is a criminal offence under this law to obstruct access to a record or destroy the information or an internal review or complaint.

If for no justifiable reason, a public officer refuses to furnish the information, a fine can be imposed by the Information Commission.

SINDH T&RTI ACT 2016

Public bodies are required to proactively disclose information and designate public information officers.

Public bodies must appoint a designated official.

If information is not provided, an applicant can file an internal review with the head of the public body or approach the information commission.

Public body must respond within 15 days or receipt of request, which can be extended for a further 10 days.

RIGHT OF ACCESS TO INFORMATION ACT 2017 (FEDERAL)

Public bodies are required to proactively disclose information and designate public information officers.

Public bodies must appoint a designated official.

Public body must respond within 10 days or receipt of request, which can be extended for a further 10 days.

An appeal against the public body lies to the information commission.

Right to Information Laws

THE BALOCHISTAN RIGHT TO INFORMATION ACT, 2021

Public body must respond within 15 days of receipt of request

A complaint can be lodged with the Information Commission if the response to a request is unsatisfactory

If for no justifiable reason, a public officer refuses to furnish the information, a fine can be imposed by the Information Commission



Justice of Peace

22-A & B OF THE CODE OF CRIMINAL PROCEDURE

If your complaint to a law enforcement agency is not entertained and they refuse to register an FIR or inquire into the case, citizens are at liberty to approach a magistrate by filing an application under 22-A/B of the CrPC.

Habeas Corpus

ARTICLE 199 OF THE CONSTITUTION OF PAKISTAN

A habeas corpus is filed under the jurisdiction of the High Court when someone goes missing. This is filed by a family member, after which the HC issues instructions to LEAs and concerned departments to recover and produce the missing individual.

Terrorism

Comment: The definition of “terrorism” under Section 6 of the Anti-Terrorist Act, 1997, has been routinely expanded to register FIRs against politicians, journalists and dissidents despite a clear pronouncement by the Supreme Court about when such an offence is or is not attracted.

Provisions of the ATA continue to be invoked against journalists to deter reporting.

Punishment: 7 years to life imprisonment and death if the action has led to the loss of life.



Promoting enmity between different groups

Explanation: Deals with promoting enmity between different groups

Comment: Uses broad language that has the effect of empowering law enforcement authorities to arbitrarily restrict freedom of expression of journalists through registration of FIRs. The language used in Section 153-A includes “by words, either spoken or written, or by signs, or by visible representations or otherwise.” The ambiguous wording - including the use of the word “otherwise” in subsection (a) of Section 153-A - poses challenges to journalists vis-a-vis reporting, particularly with respect to reporting on conflicts or ethnic/racial tensions/hostilities.

Punishment: Up to 5 years imprisonment and a fine

Statements conducing to public mischief

SECTION 505 OF THE PENAL CODE

Explanation: It deals with “any statement, rumor or report” that is made with intent to cause or incite (or which is likely to incite) any officer of the Armed Forces to mutiny; or with intent to cause (or which is likely to cause) fear or alarm to the public or induce anyone to commit an offence against the State or against public tranquility; or with intent to incite (or which is likely to incite) any class or community of persons to commit any offence against any other class or community.

Punishment: Up to 7 years imprisonment and a fine.

Comment: This section is routinely invoked against journalists and dissidents, particularly those critical of the military establishment.

Abetment of act of insubordination / Abetting mutiny or attempting to seduce sailor, soldier or airman from his duty

SECTIONS 131 AND 138 OF THE PENAL CODE

Explanation: Deals with offences relating to the army, navy and air force.

Punishment: Under Section 131, the penalties provided include life imprisonment or imprisonment up to a term of ten years, along with a fine. Section 138 provides for punishment of imprisonment which may extend to six months or with fine, or with both.

Comment: These provisions have been used against journalists independently as well as together with the criminal defamation provision contained in the Penal Code.

Contempt of court

Under Section 5 of the Contempt of Court Ordinance 2003

Punishment: Up to 6 months and/or a fine of up to Rs. 100,000.



3.2 Reporting Protocols

Cyber Harassment

Prevention of Electronic Crimes Act 2016

How to Report:

Federal Investigation Agency (FIA's) Public Complaint Portal.

Registration form: <https://complaint.fia.gov.pk/>

Cyber-crime regional offices: <https://fia.gov.pk/contact>

Process:

- 1 Filing of complaint by complainant
- 2 Inquiry for complaint initiated by the Investigation Agency i.e. FIA
- 3 Investigation process initiated
- 4 FIR is registered in light of investigation
- 5 Investigation officer submits an investigation report
- 6 Court takes cognizance of the submitted report
- 7 Charges are framed against the accused by the Court



8

Commencement of trial

- 8.1. Supply of copies to accused
- 8.2. Evidence of prosecution is generated
- 8.3. Statement of the accused is taken
- 8.4. Final arguments

9

Court issues judgment (conviction/acquittal)

Criminal Assault

Pakistan Penal Code (ACT XLV of 1860)

How to Report:

In case of a violation of Section 354 of the Pakistan Penal Code, the victim is required to file an FIR at their local police station.

The complaint for a violation of Section 509 will need to be filed before the relevant court.

Process: If filed under Section 354

1

FIR under section 154 of the CRPC lodged

2

Investigation process is initiated

3

Submission of report by Investigation Officer

4

Court takes cognizance of the submitted report

5

Charges are framed against the accused by the Court



6

Commencement of trial

- 6.1. Supply of copies to accused
- 6.2. Evidence of prosecution is generated
- 6.3. Statement of the accused is taken
- 6.4. Final arguments

7

Court issues judgment (conviction/acquittal)

Process: If filed under Section 509

1

Complainant files a complaint under Section 200 of the CPC before the Judicial Magistrate

2

Judicial Magistrate records statements of complaint on oath and orders for an inquiry
Inquiry can be undertaken by either the Police or the Judicial Magistrate

3

Inquiry report is submitted

4

Court takes cognizance of the inquiry

5

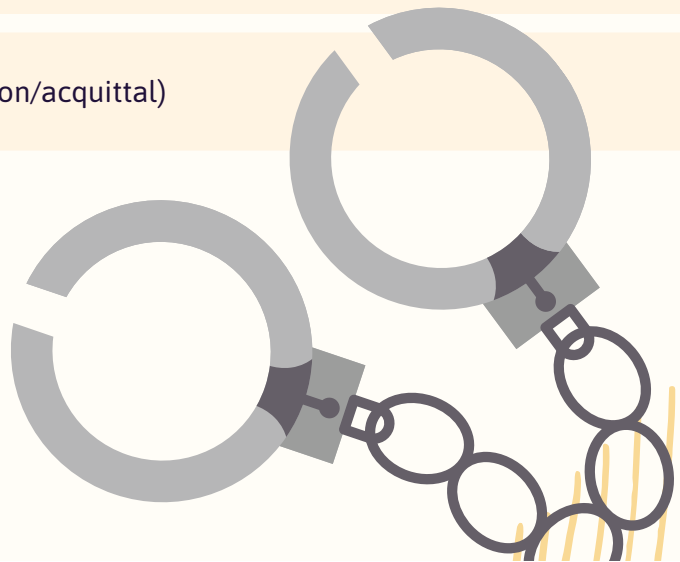
Charges are framed against the accused by the Court

6

Commencement of trial
6.1. Supply of copies to accused
6.2. Evidence of prosecution is generated
6.3. Statement of the accused is taken
6.4. Final arguments

7

Court issues judgment (conviction/acquittal)



Harassment at the Workplace

Protection Against Harassment of Women at the Workplace (Amendment) Act, 2022

How to Report:

All registered organizations are required by law to form a three member inquiry committee where the complaint can be lodged. If such a committee does not exist, then a complaint can be filed before the ombudsperson (provincial). As per law, the ombudsperson must decide the case or appeal within 90 days.

Process:

- 1 Complainant files complaint before the Office of the Ombudsman or the internal (organization) inquiry committee
- 2 Ombudsman takes cognizance & issues process
- 3 Commencement of trial
 - 3.1. Supply of copies to accused
 - 3.2. Evidence of prosecution is generated
 - 3.3. Statement of the accused is taken
 - 3.4. Final arguments
- 4 Judgment is issued



Types of Evidence that can be submitted when lodging complaint to FIR/Ombudsman/Inquiry Committee



Ocular Evidence

Any verbal evidence witnessed by the complainant directly or by other witnesses i.e. heard/saw/perceived an offence being committed



Documentary Evidence

Textual evidence i.e. email/phone conversations. If a piece of evidence has been taken from an electronic device, the complainant must ensure that the original of the evidence is also preserved in the device and not deleted



Medical Evidence

Evidence of physical or psychological harm i.e. medical reports, statements from doctor etc.



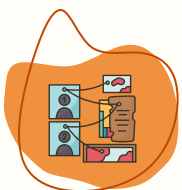
Forensic Evidence

Fingerprints, DNA evidence (if applicable) etc.



Corroboratory Evidence

All-encompassing evidence pertaining to the case at hand



Circumstantial Evidence/Evidence of Good or Bad Character

Any past details pertaining to similar offences committed by or complaints against the accused

3.3 Seeking help

If you need assistance, or your case is stuck in the legal system, there are independent organizations and commissions to provide help.

- ▶ Digital Rights Foundation has been running a cyber harassment helpline since 2016
- ▶ National Commission for Human Rights (NCHR) has launched a human rights complaint cell, which will give priority to complaints by women journalists
- ▶ Rozan has been running a free psychological counseling service for more than a decade

Digital Rights Foundation

Contact

📞 0800-39393

✉️ helpdesk@digitalrightsfoundation.pk

🐦 @DigitalRightsPK

📘 /DigitalRightsFoundation

Where to complain

- Complaints can be made through the helpline, email or social media
- The toll-free helpline number can be accessed from Monday-Friday between 9AM to 5PM

How is help available




- Case assessment
- Takedown requests sent directly to platforms
- Assistance in identifying and locating relevant FIA Cyber Crime offices and officers and workplace harassment ombudspersons
- In some cases, accompanying the complainant to FIA office
- Referring cases to relevant psychological counselors and lawyers
- Assistance to complainants in gathering evidence

Who is available

- DRF's in-house team of IT experts, psychologists and legal team for assessment for further action

National Commission for Human Rights (NCHR)

Contact

 051-9217340  complaints@nchr.gov.pk  National Commission for Human Rights
5th Floor, Evacuee Trust Complex, F-5, Islamabad
Capital Territory.

Where to complain


- Complaints can be made by a physical visit, post, or online via email, or the PM Citizen's Portal
- In-person from Monday-Friday between 8AM to 4PM
- The NCHR can also take suo moto notice of a case from the news media

How is help available

- The NCHR focal person assesses whether the case violates the complainant's fundamental rights
- NCHR issues notices to relevant agencies to ask for a report regarding the complaint
- If the complainant is not satisfied with the report of the relevant agency, the NCHR has the powers of a civil court to hear cases and dispose of them

Rozan

Contact

 0304-111-1741

Where to complain

10AM to 8PM

7 days a week

How is help available

Free telephonic psychological
counseling

Who is available

Trained team of
psychological counselors

Kinds of issues and who to go to

Mental health (psychosis or stress)	DRF and Rozan
Digital	
Account recovery, account verification, account hacking and account disabling	DRF and social media platforms - FIA
Online stalking	DRF, FIA
Doxxing	DRF, FIA, and social media platforms
Non-consensual use of images	DRF, FIA, social media platforms
Non-consensual use of explicit images	DRF, FIA, social media platforms, NCHR
Targeted and coordinated online attacks	DRF, FIA, social media platforms and NCHR
Online blasphemy accusations	DRF, social media platforms and NCHR
Online violence	DRF and NCHR
Sexual harassment	DRF and Workplace harassment ombudsperson
Impersonation	DRF, FIA, and social media platforms

3.4 Legal Checklist



Have you prepared an application that documents the incident in detail?



Have you put the evidence you have on a USB?



Do you have a paper copy of everything you are submitting?



Do you have your original CNIC?



Do you have a copy of your CNIC?



Did you get a formal receipt of your complaint?

Empowered
Women
Empower
Women

Understanding Key Concepts Through Videos



Understanding Key Concepts Through Videos

Still unsure about some of the processes and resources included in this kit? The following videos explain how to file an FIR under the cybercrime and harassment law or how to cope with stress or trauma. For more detailed information, you can always refer to the relevant sections in the resource kit.



4.1 Mental Health by Dr. Asha Bedar, clinical psychologist

Dr. Asha Bedar speaks to CEJ about how to differentiate between regular stress and symptoms that indicate it is more than just that. She provides some self-help advice you can follow to address this.

What impact can abuse, trolling and threats have on the mental health of an individual? [Click here](#)

How can a journalist facing these attacks recognize the impact it is having on their mental health? [Click here](#)

What can they do to address the negative impact on their mental health? [Click here](#)



4.2 How to report unlawful activity, abuse, and threats by Hyra Basit, Helpline Manager, Digital Rights Foundation

What are some settings you can adopt to prevent account breaches? What can you do if it happens, or if someone is misusing your data, images, threatening or abusing you? DRF provides answers.

What kind of complaints by journalists are commonly received by the DRF helpline? [Click here](#)

How does DRF facilitate journalists in i) flagging an issue with a platform through DRF ii) reporting a crime to law enforcement? [Click here](#)

What do you recommend journalists gather and communicate when they approach DRF for help? [Click here](#)

What account settings do you recommend journalists activate? [Click here](#)

What kind of problems encountered by users do platforms' community guidelines and rules cover? [Click here](#)

How can journalists active on social media report abusive content? [Click here](#)



4.3 Reporting under the law by Imaan Hazir-Mazari, lawyer

Unsure of how to seek remedy under the law? Lawyer Imaan Hazir-Mazari explains how to seek remedy and what you should do when reporting under a law.

How can an FIR be lodged at a police station? [Click here](#)

How can a complaint be filed under PECA? [Click here](#)

How can a complaint of harassment be filed before the ombudsperson? [Click here](#)

How can a complaint be filed with the journalist safety commission? [Click here](#)

What are some recommendations to complainants as they go through these processes? [Click here](#)



4.4 Trolling is a tool of gendered disinformation, Nina Jankowicz, researcher and writer

“Would they be brave enough to say these things to my face?”

Nina Jankowicz, author of *How To Be a Woman Online* and *How to Lose the Information War* on online abuse and gendered disinformation.





Annex: Risk Assessment

Digital Risk Assessment Form

A risk assessment form is structured to help journalists identify risks, threats, as well as the source of these, during the course of their work so they can take preventive measures or have a plan when something goes wrong.

Some portions of the 'mitigation' (what to do before) and 'action' (what to do after) columns have been filled in for you, but it is better to fill the digital risk assessment form yourself tailored to your story and situation.

Digital Risk Assessment Form

Part One

Outline

Outline your assignment

Before you can properly identify the major risks to your digital security, it's a good idea to break down your assignment and consider its key elements. Try to identify all the major components: the story, interviewees, travel arrangements and any other actions that are vital to your plans. Once you've done this, it will be easier to identify all the areas you need to consider for your risk assessment.

What are the stories/editorial intention	
Who will you meet	
Travel plans	
Accommodation	

Part Two

Digital Risk Assessment Form

What digital threats are posed by covering this story?

Now think about your key risks, threats and adversaries.

Remember, you don't have to be covering a controversial or sensitive story to be digitally vulnerable. You should get into the habit of completing a risk assessment for all assignments or stories, as the process may reveal potential threats that you had not already thought about.

1. Risks, Threats and Adversaries

Risk and description	Mitigation measures (Prevention)	Actions (What you can do if you, your team or your contributors are under threat)
<p>a) Will you be contacting or interviewing vulnerable people?</p> <p>If yes:</p> <ul style="list-style-type: none"> • How will you store and protect the data of people you are interviewing? • How and where will you store your notes and materials? 	<p>Use encrypted messaging services such as Signal and WhatsApp to communicate with vulnerable people</p> <p>Encrypt your devices</p> <p><i>Computer</i> – encrypt the device on your computer, which is known as full-disk encryption</p> <ul style="list-style-type: none"> • Bitlocker for Windows • Filevault for Mac <p><i>Files, hard drives and USBs</i> – Encrypt your drive and/or external devices using Veracrypt. To encrypt files in the cloud, Cryptomator is a good option.</p>	<p>Set up a remote wipe for smartphones</p> <ul style="list-style-type: none"> • Find my iPhone for iPhone • Android Device Manager – you may need to enable ‘remote lock and erase’
<p>b) Are you covering a sensitive or controversial topic?</p> <p>If yes:</p> <ul style="list-style-type: none"> • Does it involve information that needs to remain secret or confidential? • Do you understand and know how to use secure research methods? • When are you going to be at greatest risk? • When will your sources be at the greatest risk of targeted surveillance: during research or production, when the story is finished or when it goes public? 	<p>Use a VPN and incognito mode</p> <p>OR</p> <p>Use a secure browser like Brave or Tor</p> <p>Erase search history</p>	<p>Keep a backup of your information on multiple secure devices or drives</p> <p>Avoid communicating over public WiFi like the airport, cafes, government offices or malls</p> <p>Don’t use identifiable email addresses or personal communication methods</p>

Risk and description	Mitigation measures (Prevention)	Actions (What you can do if you, your team or your contributors are under threat)
<p>c) What is the location of your assignment/story?</p> <ul style="list-style-type: none"> • What is known about government surveillance/censorship of the web and mobile communications in that area? • What are the laws around the use of encryption, VPNs, or the right to free speech on social media? • What has been published regarding the persecution or rights of journalists, whistle-blowers or activists over their online activity? 		
<p>d) Who are the adversaries likely to pose a threat to your digital security? Think of your adversaries in two ways:</p> <p>i) INTENTIONAL ADVERSARIES: These could be governments, businesses, criminal organisations or individuals opposed to your work or to media exposure. Think of who may face some cost (legally, reputational, professionally, etc.) as a result of your assignment.</p> <p>ii) UNINTENTIONAL ADVERSARIES: This can include random hackers targeting a service used by thousands of people, including you. It could be someone hacking a wireless network or it could be the theft of your equipment.</p>	<p>Encrypted cloud services Journalists frequently back up documents to the cloud, using popular services such as Google, iCloud and Dropbox. These may be perfectly suitable for many users, but you should be aware that your documents are only as secure as the service they are stored on. Some of these services have been breached and user data has been stolen. If you are storing especially sensitive documents and/or material or are concerned that you might be targeted directly by an adversary, you may want to use an encrypted cloud service. Some examples of encrypted cloud services include:</p> <ul style="list-style-type: none"> • Spideroak • Tresorit 	

2. Your equipment

Risk and description	Mitigation measures (Prevention)	Actions (What you can do if you, your team or your contributors are under threat)
<p>List each piece of communications equipment you will be bringing.</p> <p>For each one, state:</p> <ul style="list-style-type: none"> • What kind of messages will you be sending and receiving with the device (e.g. SMS, email, instant message, phone calls)? • Is there, or has there been, any sensitive information on this device that could put you at risk or that you need to protect? • Will you always have your devices with you? • Will you be leaving the device where someone may be able to access it? • Do you have security checks (e.g. passwords, encryption, etc.) set up on your device to help prevent unauthorised access? • Will you be using anyone else's communications equipment or public internet access during your assignment? • What steps will you take to reduce the risk that using this equipment could pose to you? 	<p>Set up a remote wipe for smartphones</p> <ul style="list-style-type: none"> • Find my iPhone for iPhone • Android Device Manager – you may need to enable 'remote lock and erase' <p>Set up iron-clad passwords on all your devices. Use KeePass to auto generate strong passwords</p> <p>Do not use public internet to send sensitive material</p> <p>Keep your device screen clean at all times and avoid using easy patterns for unlocking</p> <p>Use a secure password manager and avoid storing sensitive information in notebooks or other material that is at risk if forgotten somewhere</p>	

3. Your materials

Risk and description	Mitigation measures (Prevention)	Actions (What you can do if you, your team or your contributors are under threat)
<p>Consider what material(s) you'll be gathering or recording during your assignment.</p> <p>For each one, list:</p> <ul style="list-style-type: none">• What format is the material (e.g. film, text, audio, images, etc)?• Is the content controversial? If it were accessed by hostile parties, would this put you or anyone else involved in the report under threat?• Where/how is this material being stored? Have you taken any steps to protect this information?• Will you need to send material?• What steps are you taking to minimise the chance and severity that recording/transmitting the material will pose?• How are you moving your material across borders?	<p>Keep a backup of USBs and memory cards with 'safe material' to show authorities</p> <p>Immediately upload sensitive material to encrypted Cloud storage</p> <p>Use SecureDrop for receiving information from sources</p>	



4. Communications

Risk and description	Mitigation measures (Prevention)	Actions (What you can do if you, your team or your contributors are under threat)
<p>List all of the people who you will need to contact while on assignment, such as interviewees, freelance colleagues, sources and editors.</p> <p>For each contact, state:</p> <ul style="list-style-type: none"> • Who are they and who could be monitoring them (employer, government, etc.)? • How will you be contacting them? Have you researched which method of contact is most secure? • Will you need to send or receive any sensitive information from them? • Will contacting them put you or anyone else at risk? What steps will you take to mitigate the chance and severity of this risk? • Do you have a plan for backing up and deleting messages? Have you discussed this plan with your source? 	<p>Don't communicate, send/receive information over public WiFi networks</p>	



5. Research and online access

Risk and description	Mitigation measures (Prevention)	Actions (What you can do if you, your team or your contributors are under threat)
<p>Think about what sites, information and content you will need to access online and consider the potential risks of doing so. If accessing online content could cause you problems, make a list to help you consider the dangers.</p> <p>For each one, state:</p> <ul style="list-style-type: none">• Have you researched the company that provides you with both your Internet and your mobile phone coverage? Do they have a close relationship with the government of the country you are living/working in?• Have you researched the law to find out how long these companies are required to keep your data on file?• Is that content blocked in the country/region you will be working from?• If you need to access blocked content, how will you do this?• What potential is there that your activity could be monitored?• What steps will you take to mitigate these risks?	<p>Use a secure browser such as https://www.torproject.org. to defend yourself against tracking and surveillance. Note: You will need a VPN. PTA issued a <u>notice for VPNs to be registered</u>.</p>	

6. Your digital profile

Risk and description	Mitigation measures (Prevention)	Actions (What you can do if you, your team or your contributors are under threat)
<p>a) Have you reviewed your online profile for content that could put you or your contacts at risk?</p> <ul style="list-style-type: none"> • Have you researched yourself online to see what information is available about you and taken steps to remove data you do not want in the public domain? • Have you published or commented on anything that criticises an adversary? • If yes, what are you going to do to mitigate the severity of this risk? 		
<p>b) Do you have one or more personal websites?</p> <ul style="list-style-type: none"> • Could the information stored on it put you or your contacts at risk? • If yes, what are you going to do to mitigate the severity of this risk? 		



Risk and description	Mitigation measures (Prevention)	Actions (What you can do if you, your team or your contributors are under threat)
<p>c) Are you planning on using social media during your assignment or story?</p> <p>If yes:</p> <ul style="list-style-type: none"> • Have you created long, strong passwords for your accounts? • How up-to-date are your privacy settings on social media sites? • Have you actively engaged in (tweeted, shared, commented, liked, etc.) content that could put you at risk while on assignment? • Do you have separate personal and work social media accounts? • What other steps are you taking to mitigate the chance and severity that your social media activity could pose to you? • Have you considered the possible psychological impact of social media on you, your team or your contributors? 		

