A RIGHTS-BASED APPROACH TO

DIGITAL SAFETY & ONLINE CONDUCT

FOR ROHINGYA REFUGEES IN BANGLADESH

TRAINING MATERIAL

Photo: Sazia Sharmin

TABLE OF CONTENTS

INTRODUCTION

While refugees are increasingly online, they remain invisible in national digital rights conversations. Current policies offer no formal protection for refugees navigating digital spaces. As a result, Rohingya individuals, from community journalists and human rights defenders to camp volunteers and youth, are left vulnerable to surveillance, exploitation, and misinformation, which breaches their freedom of expression and privacy. They interact with digital systems daily, without recognition, inclusion, or support.

This **Rights-Based Digital Safety & Security** training material was developed to change that.

With time, refugee communities have adapted to life in displacement. Families and neighbors have rebuilt informal networks of trust. Many now rely on each other—on friends, relatives, and religious leaders—to stay informed. Mobile phone use has also increased, opening new pathways to knowledge, connection, and self-expression.

Access to information and digital tools has grown significantly across the Rohingya refugee camps. According to an Information Ecosystem Assessment (IEA), building on a 2017 study by Internews and the Emergency Telecoms Sector, the number of refugees who say they have enough information to make decisions about their daily lives rose from just 23% in 2017 to 92% by 2019.

But access is not equal: women, in particular, face greater barriers to owning phones, accessing media, or benefiting from digital services. And while host communities in Cox's Bazar use more traditional media like television and radio to meet their information needs, refugees depend on word-of-mouth and mobile communications. Across both communities, meaningful communication with aid agencies remains limited, even as conditions improve. This persistent gap raises a serious question: whose voices are being heard, and whose needs are being left behind?

These realities form the backdrop of this training initiative on Digital Rights Protection of Rohingya Refugees in Bangladesh: Capacity Development and Advocacy for Policy Change.

Through day-long workshops across 32 administrative camps, this activity will equip 100 Rohingya participants with critical knowledge and tools to understand and defend their digital rights. Whether using a smartphone to connect with family, writing about your community, or advocating for justice, your digital safety matters. More than that, your right to participate, to be heard, and to access technology with dignity must be upheld.

For Rohingya youth and community leaders, claiming space in the digital world is not about convenience; it is about survival, self-representation, and sovereignty. This training is a technical intervention and a call to recognize Rohingya refugees as rights-holders in the digital age. It asserts that even without legal citizenship, they are members of a global information society, and their protection, inclusion, and leadership are essential to any just and accountable digital future.

Chapter 1
DIGITAL SAFETY AND SECURITY

In today's connected world, being online is part of everyday life—whether for staying in touch with loved ones, finding information, sharing stories, or accessing aid. But along with these opportunities come real risks. For communities like the Rohingya, who often live without legal protections and with limited access to formal education or support, understanding how to stay safe online is not a technical luxury; it is a critical survival skill.

Digital security and safety training is the first line of defense against a growing range of threats: from online scams and identity theft to surveillance, misinformation, and harassment. This chapter introduces the foundational concepts of digital safety and cybersecurity and explains how both can help individuals navigate the internet confidently and cautiously.

Digital security and safety training equips individuals with the knowledge and skills to protect themselves and their data from online threats. In contrast, cybersecurity training focuses on protecting computer systems and networks from unauthorized access and damage. Both are crucial for navigating the digital world safely and responsibly.

Digital safety and security training focuses on protecting an individual's online presence, data, and identity. Key areas include:

- Identifying and avoiding scams, phishing attempts, and social engineering tactics
- Understanding and managing privacy settings
- Practicing safe online habits, such as using strong passwords, updating software, and being mindful of what information is shared online
- Recognizing and reporting potential risks, such as misinformation, hate speech, and deepfakes

Digital safety training empowers individuals to make informed online decisions, protect their personal information, and recognize when something is suspicious. It also helps build confidence, especially among new internet users, by creating awareness about rights, responsibilities, and simple security strategies.

Cybersecurity training, on the other hand, shifts the focus to larger systems. It protects computers, mobile devices, networks, and stored data from unauthorized access, theft, or damage. Key areas include:

- Understanding cyber threats and system vulnerabilities
- Implementing technical protections like firewalls, antivirus software, and encryption
- Creating and maintaining security policies and procedures
- Responding to and recovering from cyber incidents, such as data breaches or hacking attempts

Cybersecurity helps ensure digital infrastructure's confidentiality, integrity, and availability—whether in an organization, a government office, or a humanitarian system. For example, camp

aid organizations need strong cybersecurity practices to protect refugee data and maintain trust.

Understanding the difference between digital and cyber safety is important because they deal with different kinds of protection. Knowing the difference helps people respond to problems in the right way. For example, if someone spreads rumors about you online, that's a digital safety issue. But if your data is stolen from a server, that's a cybersecurity issue. Each problem needs a different kind of solution.

These two areas are also connected. People's data can be exposed if a computer system is not secure. And if people don't know how to stay safe online, they can accidentally create risks for the system. That's why it's essential to understand both—to protect yourself and your community, and to be more confident in the digital world.

Ultimately, learning about digital safety is not just about avoiding harm; it's about empowerment. For displaced communities navigating uncertain futures, understanding how to stay safe online means gaining control over one part of their lives. It means being able to share, speak, and connect without fear.

Chapter 2
DIGITAL RIGHTS AND RESPONSIBILITIES

What Does it Mean to be a Digital Citizen?

A digital citizen is someone who has an identity on the Internet. Being a digital citizen means being part of a digital community; therefore, you must exercise self-awareness and awareness of others. Digital citizenship is accompanied by many rights and responsibilities intended to protect you and everyone with whom you interact.

Key Digital Rights

- Right to access and use computers and/or other electronic devices
- Right to access and use digital content
- Right to create and share digital media
- Right to privacy in digital communities
- Right to express your ideas and opinions freely
- Right to report anyone or anything that seems inappropriate


Maintain
Maintain your privacy. Do not share personal information, and other private information.


Create
Create a blog, wiki, or other platform to voice your opinion or findings.


Access
Only access the technology when you are suppose to. Ground rules may need to be set.


USE
Use caution when talking to people you do not know.

Chapter 3

INTERNATIONAL HUMAN RIGHTS CONCEPTS IN THE PRETEXT OF DIGITAL SECURITY AND SAFETY

Digital rights are human rights in the digital realm, encompassing access to information, freedom of expression, privacy, and security in online environments. These rights and responsibilities are increasingly recognized under international law, particularly as digital technologies evolve and impact societies. While established human rights frameworks apply online, the unique characteristics of the internet, such as its global reach and rapid dissemination of information, present new challenges and require specific consideration.

Application of Human Rights

International law, including the International Covenant on Civil and Political Rights (ICCPR), recognizes that existing human rights apply in the digital space. This includes freedom of expression, privacy, and protection from discrimination.

Digital Rights Specifics: The digital realm has also spawned new rights and responsibilities specific to the online environment. These include the right to access the internet, the right to be forgotten, and the right to data protection.

Challenges of the Digital World: The internet's global reach and rapid dissemination of information present challenges for enforcing legal principles and holding individuals accountable for online actions. For example, it can be challenging to identify an online speaker's true identity or determine jurisdiction for a claim.

Responsibilities: Digital rights come with corresponding responsibilities. These include behaving ethically and responsibly online, respecting the privacy of others, and ensuring the safe and inclusive use of digital technologies.

International Legal Frameworks: International organizations, such as the Council of Europe, play a crucial role in promoting digital rights and responsibilities at the international level. They develop guidelines, policies, and recommendations to ensure that digital technologies are used in a way that respects human rights and promotes democratic values.

State and Non-State Actors: International law also recognizes the responsibilities of state and non-state actors, such as internet service providers and social media platforms, in protecting digital rights and ensuring a safe and inclusive online environment.

Emergence of Digital Rights: Digital rights are an evolving field, with ongoing discussions about the appropriate legal frameworks and policies to address the challenges and opportunities presented by digital technologies.

Freedom of Expression

One of the fundamental foundations of any democratic state system is the guarantee of freedom of thought, conscience, and expression. Article 19 of the Universal Declaration of Human Rights (UDHR) urges citizens' right to freedom of expression. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) also calls for freedom of expression. Bangladesh is a signatory and ratifier of the ICCPR and several other international human rights instruments. Therefore, Bangladesh must abide by international human rights laws in the national and global community. Just as Bangladesh has to be constitutionally democratic, so too must any law or regulation enacted by the legislature not conflict with any international charter. Here is the expectation of the citizens of Bangladesh and the global and regional community.

Although international charters do not consider digital or online media, theoretical or objective rules for digital or online activities fall within the scope of this charter. Issues related to the concept of freedom of expression have been further clarified and elaborated by the UN Committee on Human Rights, General Comment No. 34 (hereinafter GC34) on Article 19, the resolutions adopted by the UN General Assembly, and various reports by UN Special Rapporteurs. However, according to GC34 and multiple reports by UN Special Rapporteurs, the academic goal or purpose of ensuring freedom of expression offline will also apply to ensure freedom of expression online.

Although the Bengali translation of 'Freedom of Expression' is 'Freedom of Opinion', its scope is not limited to constitutional or legal concepts. No healthy and active political sphere can be formed without freedom of thought, conscience, and expression. Various studies and international experience prove that the suppression of thought, conscience, and expression creates conditions for terrorism and violence. Freedom of expression means not only freedom of speech but also freedom of expression in any other way. Many fundamental rights, including the right to life, the right to privacy, the right to freedom of religion and belief, and the right to freedom of movement, are related to the freedom of speech and opinion. Just as ensuring citizens' freedom is necessary to establish a democratic state system, it does not mean spreading hatred or animosity towards any particular race, caste, religion, or group.

Article 39 of the Constitution of Bangladesh and Article 19(3) of the ICCPR determine why a State may restrict freedom of expression. It states that, subject to certain conditions to protect the rights or reputation of others and to protect national security, public order, public health, and ethics, the State may restrict expression. Also, the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, and the Tshwane Principles on National Security and Right to Information state that the purpose of interfering with freedom of expression must be clearly defined by law. The basis of legitimacy must be clear to the citizens as part of the State's duty to protect democracy. After all, limiting rights must not be excessive. Freedom of expression includes the right to information, store information, and provide information.

The reports of the UN Special Rapporteurs play an essential role in protecting the freedom of expression, the right to privacy, and various civil rights of citizens. A report by the UN Special Rapporteur (Frank La Rue) for the Promotion and Protection of Freedom of Expression was

presented at the 17th session of the UN Human Rights Council in Geneva in May 2011. The critical points of the report highlight the Internet as one of the most powerful tools of the twenty-first century, partly because of its unique technical features, such as bringing transparency to the behaviour of those in power, the right to information, and enhancing the benefits of active citizen participation in building a democratic society. The report reiterates that Article 19 of the UDHR and the ICCPR entirely apply to online freedom of expression.

The report also examines significant trends and challenges in the right of all individuals to seek, obtain, and disseminate information through the Internet. The Special Rapporteur emphasized the unique and transformative nature of the Internet, enabling the exercise of the individual right to freedom of opinion and expression, in many other human rights practices, and the progressive development in society. Chapter 3 of the report identifies the applicability of international human rights norms and standards to online freedom of opinion and expression as a means of communication. Several exceptions exist where disseminating certain types of information can be restricted. Chapters 4 and 5 mention two forms of internet use: a. internet access; and b. access to the material and technical infrastructure needed to access the Internet. Chapter 4 identifies explicitly some ways the States are increasingly censoring online information. These include— blocking or filtering content tenaciously, criminalizing legitimate expression, imposing intermediate liability, disconnecting users from the Internet, including intellectual property rights in the cyber law, cyber-attacks, and inadequate protection of privacy and the right to information security. The fifth chapter discusses the issue of universal internet access. The Special Rapporteur said he would investigate the matter further in his report to the General Assembly later. Chapter 6 contains the conclusion and the Special Rapporteur's recommendations on the report's main points.

To determine how much the UN member state, Bangladesh, agrees with this report, the situation of the countries now needs to be thoroughly assessed. Undoubtedly, there are many obstacles in creating a favourable environment for accessing information and exercising freedom of expression online. The Special Rapporteur's report documented these trends, highlighted their position within existing human rights legal philosophies, and made recommendations for several public and private sectors.

Universal Declaration of Digital Rights

The Universal Declaration of Digital Rights is a framework that asserts the fundamental rights of individuals in the digital realm, ensuring equal access, opportunity, and protection in online spaces. It emphasizes the importance of freedom of choice, participation in the digital public sphere, safety, security, and empowerment, especially for children and young people. The declaration also promotes solidarity and inclusion, digital education, and access to digital services, while ensuring privacy and individual control over data.

Key principles of the Universal Declaration of Digital Rights

- **Putting people at the centre of digital transformation** means that digital technologies should be designed and used to benefit individuals and society, rather than the other way around.

- **Supporting solidarity and inclusion:** This involves ensuring everyone can access digital technologies and participate in the digital world, regardless of background or circumstances.
- **Freedom of choice:** Individuals should choose how they interact with algorithms and AI systems and benefit from a fair and safe online environment.
- **Participation in the digital public space** includes the right to express opinions, share information, and engage in discussions with others online.
- **Safety, security, and empowerment:** Individuals should be protected from harm online, have control over their data, and be empowered to use digital technologies for their benefit.
- **Promoting sustainability:** Digital technologies should be used in an environmentally sustainable way that does not harm the planet.

Chapter 4
CYBER LAWS AND POLICIES IN BANGLADESH

Since 2000, Bangladesh has gradually adjusted to the Internet Age. The idea behind 'Vision 2021' and 'Digital Bangladesh has resulted in the government moving many of its functions online. Moreover, the number of people and businesses relying on technology continues to grow. Digital platforms have made paying for services easier, organizing protests, signing petitions, and writing about civic issues. However, online criminal activity has also flourished, necessitating measures to protect people.

In recent years, the Bangladesh government has passed several measures related to information and communication technology (ICT); however, these cyber laws, particularly the ICT Act 2006 and the Digital Security Act (DSA) 2018, have curtailed people's digital rights in the following ways:

- The arbitrary blocking of websites and the criminalisation of legitimate freedom of expression.
- The filtering and temporary restriction of internet content.
- The attempt to restrict online media through commercial pressure.
- The arrest, detention, and attempt to criminalise legitimate expression;
- Self-regulation and cultural norms protect against censorship;
- The lack of protection for personal data

According to Article 39 of the Constitution, citizens have the right to freedom of expression, speech, and the press. However, in recent years – and especially during the COVID-19 pandemic – the government of Bangladesh has been cracking down on these freedoms to regulate the flow of information and suppress people's ability to express their views freely. Beyond undue restrictions on civil and political rights, many people who have been detained or arrested have reported feeling socially humiliated, losing their social standing, and being concerned about being falsely accused of crimes again.

Cyber Laws in Bangladesh

On 8 October 2006, the Bangladesh parliament passed the Information and Communication Technology (ICT) Act 2006. This Act aims to create the requisite legal framework to ensure that all electronic transactions are treated equally to paper-based transactions. Sanctions for activities in cyberspace did not exist before the enactment of this law (later amended in 2009 and 2013).

In May 2015, the government began implementing a new regulatory statute, the 'Cyber Security Act', without consulting or receiving input from digital rights defenders and their organisations. The Ministry of Posts and Telecommunications adopted the "National Cyber Security Strategy" (NCSS) and Information Technology on March 11, 2014. They presented the Global Cyber Security Agenda at the International Telecommunication Union. It is written in English rather than following the Bangla Bhasha Procholon Ain 1987 (literally, the "Bangla Language Implementation Act, 1987"), which requires using the Bangla language in all records

and correspondences. Sections 9 and 10 of the NCSS mandated a plan to "Enhance Bangladesh's Cyber Laws to Address Current and Emerging Threats", necessitating the passage of new legislation like the Digital Security Act.

In 2018, the Ministry of Information and Communication Technology formulated an ICT Policy, emphasizing the need for Bangladesh to work towards establishing an ICT infrastructure to meet the country's socio-economic needs and promote innovation. The policy aims to improve vulnerable groups' access to and use of ICTs.

The Bangladesh National Assembly also passed the "Digital Security Act 2018" by voice vote, despite strong opposition from journalists, lawyers, educators, and human rights activists.

Earlier, the past Awami League government proposed three new laws, rules, and policies with the potential to pose significant risks to digital rights and the Interim Government in Bangladesh is facing considerable criticism regarding its digital rights policies, particularly concerning the Cyber Security Act (CSA) and its potential replacement, the Cyber Protection Ordinance (CPO):

1. The Data Protection Act, 2022, requires international platforms to store data locally with a national security agency headed by a government official acting as the data protection authority. Due to this arrangement, the law leaves user data originating from Bangladesh vulnerable to government abuse.
2. The Regulation for Digital, social media, and OTT Platforms 2021 mandates platforms to remove a broad range of content within 72 hours of notification and have Bangladesh-based employees ensure compliance with the law.
3. Draft of the 'OTT Content-based Service Provision and Management Policy 2021,' which will be similar to the social media and OTT Platforms regulation drafted by the Ministry of Information.

The Information and Communication Technology Act (ICT) Act, 2006

Bangladesh approved the ICT Act on October 8, 2006. It seeks to legalise all electronic data and activities. The Act addresses electronic records and signatures, their security, the institution that issues electronic certificates, the punishments for computer and internet offenses, and cyber tribunals and cyber appeal tribunals.

Chapter I of the Act covers the ICT industry and cyber regulation terms. Chapter II covers e-governance and provisions on electronic signatures. Chapter III addresses electronic record attribution, acknowledgement, and transmission. Chapter IV regulates safe electronic records and digital signatures. Chapter V governs certifying authorities. Chapter VI discusses security, digital signature certificates, private control, and acceptance. Chapters VII and VIII cover penalties, adjudication, inquiry, judgment, and punishment for several offences. Chapter VIII creates the Cyber Regulations Appellate Tribunal to review Adjudicating Officer orders.

Bangladeshis have suffered digital rights violations under the ICT Act, especially sections 46 (Power of Controller to give directions in emergencies) and 57 (Punishment for publishing fake, obscene or defaming information in electronic form). The law primarily targets journalists;

according to reports published by Prothom Alo in 2020, 46 cases against journalists have proceeded to the Cyber Crimes Tribunal over the last three years, of which only four cases were eventually dismissed. According to human rights activist and researcher Rozyna Begum, the law has also been widely used before the 2014 national election. Section 57 of the ICT Act, which criminalised online defamation and blasphemy and silenced dissenters, was of particular concern.

The ICT Act was later replaced by the 2018 Digital Security Act, which eventually repealed ICT Act Sections 54, 55, 56, 57, and 66. Interestingly, the DSA has harsher repressive penalties than repealed section 57 of the ICT ACT 2006.

Controllers' Discretionary Power

Section 46 of the original ICT Act allows the Government to order any law-enforcing agency to restrict information through any computer resource if they believe it is necessary or expedient for maintaining Bangladesh's sovereignty, integrity, or security, its friendly relations with other States, public order, or the prevention of any cognisable offence. Controllers are government-appointed. Section 46 allows a controller to offer emergency orders. Rights groups say Bangladesh has invoked Section 46 to justify website blocking and filtering.

This clause is problematic for various reasons, including the controller's vast discretionary powers. Section 46's title implies that the power should only be used in emergencies, yet it does not define emergencies. Instead, it refers to numerous broad goals, some of which are not permissible under Article 19 (3) of the International Covenant on Civil and Political Rights (ICCPR), such as preserving cordial ties with other States or deterring criminal activity. Thus, Section 46 allows a public authority (the controller) to undertake surveillance or restrict information access in many scenarios.

In addition to the difficulties described above, it is unclear why the entity governing the certification authority should have surveillance tools and the capacity to ban internet access. Law enforcement should do the first under court supervision, and the courts should order the second. Section 46's provisions violate international law and should be eliminated. If the Bangladeshi government wants to provide law enforcement or intelligence services with more monitoring capabilities, it should do so through international law-compliant legislation.

Encouraging Pre-trial Imprisonment

It is concerning that section 76 of the updated ICT Act, which bars bail for certain offenses, violates the right to liberty and may further erode the presumption of innocence required by international law. Article 9 of the ICCPR specifies that "it shall not be the general rule that persons awaiting trial shall be kept in custody," protecting their liberty and security. International law also allows states to jail people before trial merely to ensure their appearance or preserve evidence. The ICT (Amendment) Act 2013's non-bailable Section 61 offenses violate Article 9(3) of the ICCPR.

The International Criminal Court worries that lengthy pre-trial imprisonment puts individuals at risk of torture. According to human rights groups, Bangladeshi police routinely torture

detainees, as in the 2020 cases of journalist Shafiqul Islam Kajol, cartoonist Ahmed Kabir Kishore, and the late writer Mushtaq Ahmed, with Ahmed eventually dying in detention.

Immunity of the Intermediaries

The Act grants internet service providers (ISPs) immunity for any activity that breaches the Act and uses them as intermediaries. Section 79 clarifies that no network service provider shall be liable under this Act or rules and regulations made thereunder for any third-party information or data made available by him if he can show that the offense or contravention was committed without his knowledge or that he had used all reasonable efforts to prevent such crime or contravention. ISP immunity poses the risk of facilitating an increased commission of cybercrime.

Unwarranted Arrest and Criminal Procedures

The Act allowed police to undertake warrantless searches and arrests in public. Per Section 80, the Act argued that requiring a warrant for search and arrests in private places takes time and risks secrecy, and the need for warrants is replaced by a letter of consent from the relevant unit head. Warrants require a thorough legal justification for arrest and search, and eliminating such may allow for arbitrary arrests to be made on baseless allegations.

Provisions in Conflict with Public Interest Principles

According to Section 63, it is a crime to violate the ICT Act's powers or "rules and regulations made thereunder." Since this provision prevents confidential information from being disclosed without authorisation, limiting its application to public officials exercising statutory powers is permissible. The provision is troubling, however, when applied to whistleblowers who expose corruption or other serious wrongdoing. Additionally, it is unclear whether one or more private individuals could be considered "a person" who obtains information under this Act or its rules and regulations. If so, such a provision is wildly disproportionate. Additionally, this provision should be in the data protection law rather than the ICT law because it protects personal data during automated processing.

It should also be noted that Section 4 of the Public Interest Disclosure (Protection) Act, 2011, states: "Any disclosure of information may, in reasonable consideration, disclose accurate information relating to the public interest." Under Section 5 of this Act, the publisher of accurate public interest information cannot be a victim of a criminal or civil case, demotion, harassing transfer, or compulsory retirement, taking any other departmental action, discriminatory behaviour, etc., and the informant's identity must be kept secret. Thus, the current ICT Act contradicts the Public Interest Disclosure Act 2011, which must be addressed by legislative and adjudicative bodies to avoid legal confusion.

Insufficient Data and Privacy Protection

Article 43 of the Constitution states: "Every citizen shall have the right, subject to reasonable restrictions imposed by law in the interests of the security of the State, public order, public

morality or public health- (a) to be secured in his home against entry, search and seizure and (b) to the privacy of his correspondence and other means of communication."

Surveillance and national security, especially terrorism, are closely linked in Bangladesh. To protect state security and public peace, Section 97A of the Telecommunication Act of 2001 allows the government to authorise any of its authorities to record, prevent, and collect telephone communications. This provision also states that the government may request assistance from any service provider, which must comply or face penalties.

The Telecom Act allows data collection without a warrant or court order. The 2006 amendment confirms this surveillance regime. According to the Code of Criminal Procedure and the ICT Act, an investigating police officer can intercept and monitor communication and request network administrator cooperation. Anyone who refuses to help may be penalised.

Judiciary, Judges, and Unjust Justification

Section 82(1) of the ICT Act requires the government to establish one or more Cyber Appellate Tribunals to expedite and effectively prosecute ICT Act-related offenses. The government and the Bangladesh Supreme Court will choose a session judge or an assistant session judge for the cyber tribunal. The first very rapid cyber-tribunal was established in Dhaka in 2013. By April 2021, the government had established cyber tribunals in all seven divisions to hear cybercrime cases, including those filed under the Digital Security Act.

One needs a deep understanding of computer applications in information technology to resolve issues under IT laws. The tribunal must understand digital signatures, cryptography, and IT developments. It is recommended that the government ensure that a technical member (with a computer science background) is part of the tribunal to ensure that correct IT concepts are applied. The ICT Act, however, does not specify any requirements regarding ICT understanding for the selection of tribunal judges, raising concerns from digital rights activists, professionals, and lawyers over the qualifications of judges appointed to such tribunals.

Cyber Safety Ordinance 2025

In May 2025, Bangladesh's interim government introduced the Cyber Security Ordinance 2025 to replace the Cyber Security Act 2023, which replaced the controversial Digital Security Act (DSA) 2018. According to official statements, the ordinance is intended to fix flaws in previous laws, address cybercrime, and protect citizens' digital rights.

Bangladesh's journey to the Cyber Safety Ordinance began with the 2006 ICT Act, which introduced digital offences but was criticized for vague provisions. The most controversial section, 57, became a key feature of the Digital Security Act 2018, which replaced the ICT Act but was condemned for criminalizing online expression.

The DSA led to hundreds of arrests, especially targeting journalists and activists. In response to sustained public and international pressure, the government introduced the Cyber Security Act in 2023 with modest reforms, but retained many problematic provisions. The 2025

ordinance marks a further step to reform digital law, with a greater focus on rights and more precise limits on prosecutable speech, though significant concerns remain.

What the Ordinance Covers

The ordinance defines cyber offences and outlines punishments, enforcement powers, and new digital rights. Key highlights include:

- **Recognition of Internet Access as a Right:** For the first time in Bangladesh, uninterrupted internet access and data privacy are civic rights.
- **Criminalization of Online Harms:** Cyber violence, such as online sexual harassment, non-consensual sharing of intimate content, child sexual abuse material, online gambling, and religious hate speech that incites violence, is criminalized. Offences involving emerging technologies (e.g., misuse of artificial intelligence) are newly defined.
- **Governance Framework:** The ordinance establishes a National Cyber Security Council and a dedicated agency to oversee implementation. The Director General may order content takedowns through telecom regulators. However, critics argue that the law lacks independent oversight and uses vague criteria like threats to "national unity" or "religious values."
- **Law Enforcement Powers:** Police can search and arrest without a warrant for certain offences. Detainees must be brought before a magistrate promptly, and investigations can be extended up to 105 days. Penalties for cyber offences range up to 10 years in prison and fines of Tk 1 crore, slightly reduced from prior laws.

Key Legal Changes Compared to Previous Laws

The ordinance removes or modifies several clauses that were widely misused under the DSA and CSA:

- **Repeal of Nine Controversial Sections** included criminalizing criticism of the Liberation War and the Father of the Nation. Approximately 95% of existing cases under the DSA/CSA are set to be withdrawn.
- **End of Criminal Defamation:** The infamous clause allowing arrests for "defamatory" speech has been repealed, a win for journalists and activists.
- **Speech-Related Offences Narrowed:** Provisions like "hurting religious sentiment" have been reworded to focus on incitement and require clear elements like hacking.
- **New Safeguards:** Only affected persons or the state can initiate cases, reducing the risk of politically motivated or third-party complaints.

Mixed Reactions and Remaining Concerns

Civil society groups, digital rights organizations, and journalists have welcomed reduced speech-related offences and the affirmation of digital rights. However, many remain cautious. Key concerns include:

- **Vague Terminology:** Terms like "cyberbullying," "obscene," and "offensive" remain undefined, leaving room for broad interpretation and misuse.

- **Potential for Abuse:** Although criminal defamation is gone, the new "cyberbullying" offence could be misused to target journalists and online critics.
- **Opaque Process:** Stakeholder consultation was rushed, and some provisions are seen as repeating past patterns of repression.
- **International Watchdogs:** Groups like ARTICLE 19, Human Rights Watch, and Amnesty International stress that renaming laws isn't enough. They call for more precise definitions, independent oversight, and alignment with global human rights standards.

The ordinance presents a mixed picture: it offers meaningful reforms like case withdrawals and rights protections, but retains enforcement tools and ambiguous language that could still be abused. Human rights defenders should monitor how the law is implemented, especially in content takedowns and internet restrictions, arrests without warrants, and definitions of offences like cyberbullying or religious offence. Continued advocacy is crucial to push for further reforms, demand independent oversight, and ensure that digital governance in Bangladesh strengthens rather than suppresses civil liberties.

Chapter 5

ADVERSARIAL OR CONFRONTATIONAL SOURCES

Using the internet or mobile devices can sometimes expose you to risks, mainly if you communicate with people you don't fully trust or access sensitive information. Your phone or internet use can reveal personal details like your identity, location, or email address, making you vulnerable to harassment, scams, or surveillance. That's why it's essential to protect yourself before reaching out or sharing anything online. Digital safety is not just about tools—it's about thinking ahead and staying aware.

Before starting your online work

- Search your subject to see if they have a history of harassing journalists who report on them and whether the risks are digital, physical, or both.
- Review safe online research practices below before you visit a subject's website or another digital platform, such as chat rooms or Facebook groups.
- Discuss your story and its risks with your editor to find out what support will be available as you investigate and publish it.
- Conduct a review and update it regularly throughout your investigation.
- Weigh the risk of investigating the story against the reward. Is the risk significant?
- For the story, purchase a separate phone, SIM card, or virtual phone number from a service like Google Voice. Review the safer communications section below.
- For very sensitive stories, consider using Tails, a portable, secure operating system for any computer. Seek help from a security specialist to set it up.
- Imagine someone searching online for data that they can use to harass, intimidate, or discredit you. Review your profiles to see what is in the public domain and remove what you can, as detailed below.
- Be aware that sources may keep or record communications with you, including phone calls, and could make them public, present them out of context, or otherwise manipulate them.
- Step up security measures when contacting sources and immediately after publishing, when you will be most at risk.

Conducting safer research online

- Use a VPN when researching online and downloading documents, especially when viewing sites run by groups that harass the press. A VPN hides your IP address so the website owner can't see where the device you're visiting from is located.
- Use the Tor browser, the most secure way to browse the internet anonymously available right now, for your most sensitive research. Digital security specialists can assist if you need.
- Confirm that the websites you visit are encrypted, as shown by a lock icon in the navigation bar of your browser and a web address that starts with https. Unencrypted sites are insecure and leave your device vulnerable to malware.

- Use uBlock Origin for Chrome or Firefox to protect yourself from advertising that could be used to track you or install malware, and the uMatrix plug-in for Chrome or Firefox controls how your browser communicates with the sites you visit.
- Create dedicated social media accounts instead of personal accounts when joining groups run by people who might wish you harm. Use a service like Twilio or Google Voice in the U.S. to mask your real phone number when setting them up. Revealing your name or other identifying data, such as your date of birth, on these accounts increases the risk of harassment, and many journalists use generic photos appropriate for the group they are connecting with instead of their own.
- Use a throw-away email address when registering with sites that could put you at risk.
- When interacting, be extra careful not to give away personal information or click on links that might be compromised.

Creating a throw-away email

When choosing a new email for a single purpose, such as registering with a website or contacting sources:

- Use words or references that are popular with the community. Connect to chat rooms via a VPN before joining to see how others represent themselves.
- Only use the new email address to contact a particular online community.
- Please do not include anything personal, like your phone number, regular email addresses, date of birth, or location, when creating the email account, or link it to social media accounts showing your real identity.
- Erase all information and delete the account when you have finished your research. Remember to back up any communications that you will need.

Securing your online data

General best practice

- Turn on two-factor authentication (2FA) for all accounts, including financial ones like shopping websites.
- Create long, unique passwords for each account and store them in a secure password manager.
- Prioritize protecting data that can be used to locate, contact, or steal your identity, such as your home address, personal phone number, and passport number.
- Set regular calendar reminders to look yourself up online, and do so on a range of search engines using private or incognito mode. Note that you could make anything private or remove it.
- Sign up for Google alerts to be notified when others use your name online. Include common misspellings of your name, address, and other personal information you feel would be helpful.
- Sign up for a credit monitoring service to alert you if someone is seeking credit in your name.

Removing data

- Make content private on sites and accounts you own.
- Ask family and friends to remove information from sites and accounts they control.
- Be aware that it may not be possible to remove data stored on sites owned by third parties, such as public databases, and that deleted data may live on in screenshots or internet archive sites such as the Wayback Machine.
- Ask Google Maps, Apple Maps, and other companies to blur or remove your home or other identifying information.
- Ask Google Search to remove links from public search results, including links detailing personal data, such as your home address. Results on other search engines will not be affected.
- Contact the creator of the public database, usually a government body, to see if your information can be removed or made private. Laws about this differ by country.
- Services exist to help you remove your information from sites that trade data for advertising and other purposes, though it can take a month to see the effects. One example, DeleteMe, owned by the company Abine, operates in the U.S. and some other countries.

Securing your social media accounts

- Create separate accounts for work and personal use to help contain security issues in one area of your life.
- Check privacy settings regularly, as they are subject to change. Access your profile from a private or incognito mode browser to see what is public.
- Remove personal information such as your date of birth or where you went to university, which others could use to impersonate or investigate you.
- Turn off your location and any geo-tagging functions that show where you were for specific posts if the information could put you or others at risk.
- Verify your accounts, if possible, in case fake accounts appear in your name.
- Move conversations to Signal or WhatsApp, rather than direct messaging, and only use the dedicated phone and SIM card you have bought for your research.
- Think about what you post. Don't share pictures of your office, a hotel, or something else that gives away your location.
- Ask family and friends to avoid posting information and photos of you. Discuss what they share online and whether it could put you or them at risk.

Safer communications

- Buy a separate phone and SIM card to contact your sources, and don't use your personal or work phone. This protects your identity and helps separate you from subjects involved in illegal activities.
- Disguise your phone number with a virtual one from Google Voice (U.S.) or Twilio if you cannot buy a new one.
- Use a throw-away email address on the phone to prevent your research from syncing with personal or work accounts via the cloud, especially if you could be sent something illegal.

- Keep photos of yourself off the device.
- Use apps with end-to-end encrypted messaging, such as Signal or WhatsApp, to communicate, since calls and SMS messages exchanged over mobile phone networks are not encrypted, and governments and others can access the content. Be aware that a government could subpoena WhatsApp to access the metadata attached to specific accounts, such as when you created it and which other accounts you talk to; Signal stores much less.
- Secure Signal or WhatsApp accounts with advanced security features if needed, such as screen lock, registration lock, disappearing messages, and "view once" photos and videos.
- Use Wire to communicate where possible, since you can sign up without a phone number.
- Create a plan to back up and delete content stored in the apps and on the phone. Consult a digital security professional if needed.
- After publication, back up anything you need, then delete everything stored in the accounts and the accounts themselves. Disconnect the phone number and factory reset the phone.

Receiving and managing documents

- Use DangerZone to scan files received from a source for malware and convert potentially dangerous PDFs, images, and other documents into safe PDFs.
- Remember that almost anything you do on a device leaves a trace, and IT experts can recover deleted content even if you have used specialized software to scrub your computer.
- Send documents under 100MB via Signal or another end-to-end encrypted service.
- Send documents over 100MB using OnionShare.
- Be aware that metadata in documents, files, and messaging apps, such as when a document was sent, is not always encrypted and could help someone identify you and your source.

Chapter 6
USING ONLINE PLATFORMS SAFELY AS A HUMAN RIGHTS DEFENDER

Human Rights Defenders use various online platforms to distribute their work and communicate with sources and audiences. Platforms that allow interaction with others, like social media, wikis that will enable collaborative editing, or content hosting services like WordPress and Substack, can all present security issues for you and others in your networks. There are, however, steps you can take to protect yourself better.

Protect your accounts

Turn on two-factor authentication (2FA) for all accounts that allow it. This added layer of security helps prevent unauthorized access by requiring anyone who enters your password to provide a second layer of verification, often a code generated on your phone or a security key you carry with you.

- An authenticator app, such as Authy, can be used for 2FA instead of SMS, which is easier to intercept.
- Some platforms notify you of login attempts as a form of 2FA – ensure this feature is activated on each service you use.

Create long, unique passwords of at least 16 characters. Include numbers, letters, and symbols to make it harder to crack.

- Never repeat your password on different accounts. If someone compromises one password, you can still prevent them from gaining access to others.
- Never use personal information that is easy to discover as your password, such as your date of birth or your pet's name.
- Use a password manager to create and store passwords.
- Password security is even more critical for accounts that don't offer 2FA.

What you share: Private vs public

Content that you post privately might not be as private as you think. Other people on the platform – or people who work for the company that runs it – may be able to see it. Be mindful of the following:

- Think about who has access to the platform you are using. Can the public view the content? By other people with an account? Or only people you have explicitly authorized?
- Review privacy settings on each platform you use to check what is public by default. Hide, restrict, or take down content you are uncomfortable having in the public domain.

- Remember that others can access private messages and emails unless they are end-to-end encrypted, and even those can still be read by someone with access to your device, either in person or by remote hacking.
- Think carefully about what you post before you publish, since it may be permanent. Some platforms archive content even after it is deleted, which government agents can potentially request, and internet archives or other sites may also keep a record.

Personal data

Online platforms collect a lot of data about you that other people, including government officials, can access and use to surveil and harass you.

- Avoid publishing personal information that could be used to locate, contact, or verify your identity, such as your date of birth or phone number.
- Avoid publishing personal information that could reveal the identity of others, especially your sources.
- Delete content you no longer want publicly available or ask the platform to take it down. Services have different procedures – social media platforms allow you to remove some content yourself, while others, such as Google Search, Google Maps, and Wikimedia, accept requests for content to be taken down.
- Be mindful that your Internet Protocol (IP) address, which links your device to an internet connection, may be visible to website administrators, internet service providers, and others, and can be used to locate you physically.

Images

Images that you post online can give away a lot of information.

- Remove metadata, also known as EXIF data – the information attached to digital photos that reveals when and where they were taken, and with which camera or phone – before posting, if possible. Do not upload any more data than is necessary.
- Use generic, neutral profile pictures that don't reveal your face or location if you have concerns about your safety.
- Be aware that the photos you upload may be freely available for others to use under the terms and conditions of some platforms. Avoid uploading images you do not want others to share or copy, especially if they involve sensitive events such as protests and demonstrations.

Read transparency reports

Tech companies and other organizations release regular transparency reports about the requests they receive from governments to access or remove data, which can help inform your decisions about which services are safe for you to use. Examples include Google, Facebook, Twitter, Wikimedia, and WordPress.

Chapter 7
WAY FORWARD

To be a digital citizen in a refugee camp is to live in two worlds simultaneously: one where you are physically constrained, and one where you are digitally free, but exposed. You may not have citizenship in a state, but still participate in a global digital society. That society does not always protect you, but you have the right to demand that it should.

This dual existence comes with unique burdens. You face legal invisibility, statelessness, and restricted mobility. Yet the smartphone in your pocket connects you to the world: to educational opportunities, to diasporic networks, to journalists and advocates, and to platforms where your story matters. But it also connects you to threats of surveillance, misinformation, harassment, and exploitation. Navigating this dual reality requires more than just tools. It requires critical thinking, courage, and community.

Digital security isn't just about technical skills—it's a fundamental human right. For young people in the Rohingya camps, staying safe online is not a luxury but a necessity. This guide has equipped you with practical tools—from strong passwords to safer communication practices—to help you protect your identity and make informed choices in a digital world not built for your safety.

You also explored how international law affirms your rights to expression, privacy, and information, regardless of citizenship. Frameworks like the Universal Declaration of Digital Rights highlight inclusion, safety, and empowerment as essential to digital participation.

Finally, you examined Bangladesh's evolving cyber laws—from the ICT Act to the current Cyber Safety Ordinance. While the new ordinance introduces some positive reforms, it retains vague and potentially harmful powers. Understanding these risks is crucial, especially when your online voice challenges injustice or speaks for your community.

Yet this document is not just about risks. It is about building resilience. And that resilience starts with you. So, where do you go from here? Start with what is in your hands:

- ✓ **Secure your accounts and devices**. These are not just phones or apps; they are your digital homes. Lock the doors.
- ✓ **Be cautious but not afraid.** Fear can paralyze, but awareness empowers. Recognize risks, then act wisely.
- ✓ **Support each other.** No one defends rights alone. If you know something that can help others, share it. If someone is being harassed online, offer support or report it together.
- ✓ **Tell your story on your terms.** Refuse to be spoken for. Learn how to share your message safely, ethically, and creatively.
- ✓ **Stay informed.** Laws change. Platforms change. Risks change. Stay connected with digital rights organizations, training sessions, and updates, even if they come through a WhatsApp group or a community bulletin board.

- ✓ **Imagine alternatives.** What would a safe, inclusive, and empowering internet look like for you and your community? Your ideas matter, and they can influence how policies and platforms evolve.

Finally, you are not just "using" the internet but shaping it. Every time you resist misinformation, every time you support a friend facing online harassment, every time you demand privacy, every time you tell your story on your terms, you are making the internet a more just place.

The odds are stacked against you. You live in conditions of displacement, under policies that often deny you formal protections. But you also carry a powerful form of knowledge: lived experience of exclusion, resilience in crisis, and the will to survive and speak even when denied a voice. That makes you dangerous to those who profit from your silence. And it makes you essential to any future where technology is used ethically, inclusively, and justly.

Remember, even if your rights are denied on paper, they are still yours to claim. Even if the system is flawed, you can still speak, resist, and rebuild. You are part of a global movement of people who believe in dignity, rights, and justice, online and offline. Keep learning. Keep questioning. And above all, keep demanding a digital world where your identity, voice, and future are safe, protected, and free.