accountabilitylab
PAKISTAN

POLICY BRIEF

Digitisation and Public Service Delivery

What to Know and Do

/accountlabpk   pakistan.accountabilitylab.org

Contents

Executive Summary

In today's interconnected world, the integration and utilization of digital tools are crucial across all fields of work. This policy brief aims to provide a comprehensive overview of the relevant laws, best practices for digital usage, and the policies that organizations should implement to effectively adopt digital tools. It also explores how digitisation can enhance transparency, access, and public service delivery, offering recommendations to overcome the challenges that impede progress.

The first section of the policy brief delves into the legal framework governing digitisation, focusing on the Prevention of Electronic Crimes Act 2016[1], and the Right to Information Act, 2017[2]. It also discusses the proposed Personal Data Protection Bill, 2023[3]. This section outlines the obligations and liabilities under these laws, providing a clear guide on the proper use of digital devices and platforms, ensuring legal compliance and safeguarding against potential legal pitfalls.

The second part of the policy brief offers detailed guidance on digital usage and the handover of digital responsibilities within organizations. It includes essential guidelines on maintaining a clear record of who has access to various digital tools and who is authorized to use organizational devices and accounts. This section provides a comprehensive checklist of dos and don'ts to ensure secure and efficient digital practices, promoting accountability and reducing the risk of unauthorized access or misuse.

The third section of the policy brief explores how digitisation can significantly enhance public service delivery. It highlights the potential of digital tools to improve the efficiency, transparency, and accessibility of public services, thereby fostering greater trust and engagement between the public and service providers.

The final section identifies the various hurdles that can impede the digitisation process, such as technological, financial, and human resource constraints. It provides practical recommendations to address these challenges, advocating for targeted investments, capacity building, and the establishment of robust digital infrastructure. These measures aim to create a conducive environment for successful digitisation, ultimately driving progress and innovation in public service delivery.

Applicable Laws

The Prevention of Electronic Crimes Act, 2016

The Prevention of Electronic Crimes Act (PECA), 2016, colloquially referred to as Pakistan's cybercrime law, is the primary legal framework that applies to all online activity. It is a criminal law and carves out various offences. Sections 3-26 of the Act outline these offences.

Offense	Punishment
3. Unauthorized access to information systems or data	Imprisonment of up to three months or a fine of up to fifty thousand rupees or both
4. Unauthorized copying or transmission of data	Imprisonment of up to six months or a fine of up to one hundred thousand rupees or both
5. Interference with information systems or data	Imprisonment of up to two years or a fine of up to five hundred thousand rupees or both
6. Unauthorized copying or transmission of critical infrastructure	Imprisonment of up to three years or a fine of up to one million rupees or both
7. Unauthorized copying or transmission of critical infrastructure	Imprisonment of up to five years or a fine of up to five million rupees or both
8. Interference with critical infrastructure information systems or data	Imprisonment of up to seven years or a fine of up to ten million rupees or both
9. Glorification of an offence	Imprisonment of up to seven years or a fine of up to ten million rupees or both
10. Cyber terrorism	Imprisonment of up to fourteen years or a fine of up to fifty million rupees or both
11. Hate speech	Imprisonment of up to seven years or a fine or both
12. Recruitment, funding, and planning of terrorism	Imprisonment of up to seven years or a fine or both
13. Electronic forgery	Imprisonment of up to three years or a fine of up to two hundred and fifty thousand rupees or both
14. Electronic fraud	Imprisonment of up to two years or a fine of up to ten million rupees or both
15. Making, obtaining, or supplying devices for use in offense	Imprisonment of up to six months or a fine of up to fifty thousand rupees or both
16. Unauthorized use of identity information	Imprisonment of up to three years or a fine of up to five million rupees or both
17. Unauthorized issuance of SIM cards etc.,	Imprisonment of up to three years or a fine of up to five hundred thousand rupees or both
18. Tampering, etc of communication equipment	Imprisonment of up to three years or a fine of up to one million rupees or both
19. Unauthorized interception	Imprisonment of up to two years or a fine of up to five hundred thousand rupees or both
20. Offences against the dignity of a natural person	Imprisonment of up to three years or a fine of up to one million rupees or both
21. Offences against the modesty of a natural person	Imprisonment of up to five years or a fine of up to five million rupees or both With respect to minor imprisonment of up to seven years and with a fine of up to five million rupees For previous convictions with respect to a minor imprisonment of up to ten years and with a fine

22. Child pornography	Imprisonment of up to seven years and with a fine of up to five million rupees or both
22A. Online grooming, solicitation, and cyber enticement	Imprisonment of up to ten years and not less than five years with a fine of up to ten million rupees but not less than five hundred thousand rupees
22B. Commercial sexual exploitation of children	Imprisonment of not less than fourteen years and may extend up to twenty years with a fine not less than one million rupees
24. Cyberstalking	Imprisonment of up to five years or with a fine of up to ten million rupees or both
24A. Cyberbullying	Imprisonment of up to five years but not less than one year and with a fine of up to five hundred thousand rupees but not less than one hundred thousand rupees
25. Spamming	Imprisonment of up to three months or with a fine of fifty thousand rupees which may extend up to five million rupees or both
26. Spoofing	Imprisonment of up to three years or with a fine of up to five hundred thousand rupees or both

The Federal Investigation Agency (FIA) was designated as the investigation agency under Section 29 of PECA'16, to investigate and prosecute crimes under the Act. Through amendments introduced in 2023, the police, in addition to the FIA, were also given powers to take cognizance of offenses under the Act.

In 2024, a notification was issued creating the National Cyber Crime Investigation Agency (NCCIA), [4]replacing the FIA and designating the NCCIA as the investigation agency under Section 29, to investigate and prosecute offences under PECA'16. However, the FIA was, in the same notification, allowed to perform functions up to a year until the agency was fully functional. There has been no notification to this effect yet, the FIA is still performing its functions as before. According to recent news reports, a National Forensics and Cybercrime Agency is also being established.

Currently, there are fifteen cybercrime reporting centers under the FIA in various cities. To register a complaint, the affected person must file a written complaint and provide links, screenshots, etc. Once a complaint is filed and verified, the complainant will be required to record their statement and appear in court.

There are three cognizable sections in PECA'16 which means that for these offences the FIA can directly register an FIR and investigate. However, the procedure for all other offences requires them to first seek a magistrate's permission from the special PECA'16 court and then proceed. The Prevention of Electronic Crimes Investigation Rules 2018 defines this procedure in more detail.

Under the Act, for search and seizure, disclosure of content data, and real-time monitoring, a warrant/court's permission is required, but in practice, warrants are not obtained. Instead, cognizable sections of the law are used to register FIRs, proceed with arrests, and gain access to devices and data. The law requires a chain of custody requirements to be fulfilled and at the time of seizing a device a seizure memo has to be signed by the person seizing on behalf of the FIA as well as whose device is being seized. This is included as evidence during the trial.

For blocking and removal of content, the Pakistan Telecommunication Authority has been authorized to do so under Section 37 of PECA'16. The nature of some of the requests sent by the PTA to platforms are recorded in their transparency reports. Many restrictions such as the blanket banning of platforms have been the subject of litigation before various High Courts.

Alternatively, content on social media platforms can be reported to the platforms directly under their community guidelines or rules, using their reporting mechanisms. If there is a violation, this sometimes results in the suspension of posts, accounts, or certain restrictions against the accounts.

Right to Information Act, 2017

Under Article 19-A of the Constitution, federal and provincial Right to Information laws have been enacted. These seek to enable citizens' access to information by filing requests with public bodies. The laws specify time frames within which the requests must be complied with, outline certain obligations upon public bodies, and outline a process for redress of grievance if the public body does not respond to a right-to-information request. At the federal level, it is the Right to Information Act 2017 that is applicable. Under the Act, public bodies have certain obligations regarding the disclosure of information. For instance:

- Is the organization compliant with Section 5’s obligations under the Right to Information Act, 2017, as a federal, public body? (The respective section is copied below for the related details)

> 5. Publication and availability of record. (1) The principal officer of each public body shall, within six months of the commencement of this Act, ensure that the following categories of information and record are duly published including uploading over the Internet in a manner which best ensures that these are accessible subject to reasonable restrictions based on limited resources: -
>
> (a) description of the public body's organisation and functions, duties, powers and any services it provides to the public, including a directory of its officers and employees, indicating their duties and functions and their respective remunerations, perks and privileges;
>
> (b) statutes, statutory rules, regulations, bye-laws, orders and notifications, etc. applicable to the public body disclosing the date of their respective commencement or effect;
>
> (c) substantive or procedural rules and regulations of general application evolved or adopted by the public body, including any manuals cr policies used by its employees;
>
> (d) relevant facts and background information relating to important policies and decisions which have been adopted, along with a statement of the policies adopted by the public body and the criteria. standards or guidelines upon which discretionary powers are exercised by it;
>
> (e) the conditions upon which members of the public can acquire any licence, permit, consent, approval, grant, allotment or other benefits of whatsoever nature from any public body or upon which transactions, agreements and contracts, including contracts of employment which can be entered into with the public body, along with particulars about the recipients of any concession, permit. licence or authorisation granted by the public body;
>
> (f) a description of its decision-making processes as defined in the Federal Government's Secretariat Instructions, 2004 and any instructions for the time being in force for public to provide input into or be consulted about decisions;
>
> (g) detailed budget of the public body, including proposed and actual expenditures, original or revised revenue targets, actual revenue receipts, revisions in the approved budget and the supplementary budget;

(h) the methods whereby information in the possession or control of the public body may be obtained and the prescribed fee required along with the name, title and contact details of the designated officials:

(i) reports including performance reports, audit reports, evaluation reports, inquiry or investigation reports and other reports that have been finalised;

(j) such other matters which the principal officer of the public body deems fit to be published in the public interest;

(k) such other information as may be prescribed; and

(1) camera footages at public places, wherever available, which have a bearing on a crime:

Provided that if the information or record pertains to a period earlier than the year 2008, the same shall be published within reasonable time.

- Is a computerized record of disclosure under Section 5 available?
- Is there a designated official/principal information officer to handle information requests?

Personal Data Protection Bill

Pakistan does not currently have a data protection law, however, there is a draft bill under discussion that could be enacted and will place obligations upon everyone processing the data of citizens. Many tech companies that work with international clients tend to follow requirements laid out in the General Data Processing Regulation (GDPR) to meet compliance requirements.

The purpose of any good data protection law is to provide an individual with autonomy over their data and ensure privacy protection. If you collect, store, or process data in any manner or form, instituting recommended best practices is the recommended approach, especially since a data protection law is imminent. These practices, for instance, cover questions such as:

- What data do you collect?
- How is the data collected, stored, and used?
- From whom is it collected and for what purpose?
- Is the person you are collecting data from aware of the data being collected and its purpose?
- Has the person whose data you are collecting consented to its collection and use?
- Who has access to this data within the organization?
- How is the data kept secure and confidential?
- For how long is the data stored?
- Is there a data deletion policy?
- What happens in the event of a data breach?

While there is no applicable data protection law at the moment, awareness of data collection and usage at an organizational level is necessary to maintain best practices vis a vis confidentiality and privacy. [5]When a law is enacted, legal obligations will flow which will require compliance. Having a baseline knowledge beforehand will help create institutional understanding and eventual compliance.

Digital Use and Handover Policies

It is imperative for an organization to have a digital use and handover policy[6]. This enables employees to understand the practices they must adopt when using devices and social media platforms for work purposes. Be it for devices provided or presence on platforms. All of this should be guided by a written policy that clearly outlines:

- Who has access to email and social media accounts?
- Who is permitted to access accounts, post and respond?
- Who vets the communication or post before it is initiated or published?
- Are there guidelines regarding how to respond or what to post?
- How is a violation of policy dealt with?

Due to legal frameworks and liabilities, it is important also to know:

- In whose name is the Internet connection registered in?
- In whose name is the device registered (in the case of a phone)?

Any trace in response to a law-enforcement request will first lead back to an Internet connection (based on IP) and then the associated device, and by default, the person in whose name these are registered will be the first one to be questioned and held accountable.

In case the device or account of an employee managing social media on behalf of the organization is compromised (due to theft or breach), or if an employee managing social media accounts leaves employment, make sure that:

- Their access to email and social media accounts is revoked
- Passwords and any associated numbers with accounts are changed
- Others in the organization are informed

In addition, basic digital hygiene should be undertaken, which means:

- Accounts should have different and strong passwords
- 2FA should be activated for all accounts
- Back-up information should be there for recovery
- Anti-virus scans should be run frequently on all devices
- Be careful when clicking on links and downloading files

In addition to having policies for use and handover in writing, sessions with employees to communicate and review the efficacy of these policies are recommended. While having someone to manage the technical infrastructure and ensuring basic digital hygiene may be the easier thing to do, the editorial side can be challenging, especially those tasked with public engagement through social media platforms or direct contact. Editorial decisions become judgment calls at a given time and can also result in consequences if they go wrong. Therefore, an understanding and discussion through conversation to supplement any written code is a good exercise to undertake for clarity.

Public Service Delivery

For any organisation that deals with public service delivery of any kind, being visible matters. But with visibility, accessibility is also important.

- How can people reach you?
- How do they stay informed about what you do?
- Do you put out public service messages?
- How do you communicate publicly? Through what mediums?
- Is there a broadcast list?

Typically, an organization will have a website, social media accounts, and a mode of communication via a helpline or phone number. Having these and keeping them up to date by actively managing them is a good practice. If the organization deals with customers or consumers, establishing helplines or helpdesks with automated systems that provide complaint numbers and updates, is a good practice.

In addition to automation, however, the human interface helps with trust building. Given the literacy levels, facilitation despite automation will still be required. Any automated messages will also need to be bi-lingual at the very least - in English and Urdu.

Seeking input through questionnaires is helpful for the organization internally. Whether a public or private sector organization, if deals with the public, the following should be clearly outlined:

- Role and mandate
- Who to contact and how to contact
- What to do in case of an issue

In an age where misinformation and disinformation are rampant, one of the ways to correct this is by putting out accurate information and correcting inaccuracies pertaining to the organization, through a press release or statement via the organization's website and social media accounts.

Recommendations

To truly harness the potential of digitization for ease of communication, business, and public service delivery, the provision of stable and quality connections must be ensured in addition to the certainty of access to platforms used to communicate and brand. The biggest setback is the ad hoc policy-making in this sector where sometimes Internet services are completely disrupted or access to platforms is restricted indefinitely. Reduced Internet speeds impact engagement and participation, removing Pakistanis from the global stage. These significantly impact communication, service delivery, image, and investment.

Stable and Quality Internet Connections:

- **Importance**: Reliable internet connectivity is fundamental for various sectors, including communication, business operations, education, and public services. A stable connection ensures seamless access to information, services, and global networks, which is essential for the country's economic and social development.
- **Challenges**: Frequent disruptions, slow internet speeds, and regional disparities in connectivity hinder effective communication and limit participation in digital platforms. This can result in lost opportunities for businesses and individuals alike.
- **Recommendations**:
  - Invest in upgrading and expanding the internet infrastructure across urban and rural areas.
  - Implement policies that promote competition among internet service providers to improve service quality.
  - Establish regulatory frameworks that ensure consistent and reliable internet services without arbitrary disruptions.

Access to Communication Platforms:

- **Importance**: Platforms like social media, email services, and collaboration tools are critical for communication, branding, and outreach. These platforms enable businesses to market their products, engage with customers, and build their brand identity.
- **Challenges**: Restrictions or bans on certain platforms, either temporarily or indefinitely, disrupt communication and branding efforts. This affects the ability to reach a wider audience and hampers international collaboration.
- **Recommendations**:
  - Develop clear guidelines for the regulation of digital platforms to prevent arbitrary bans.
  - Ensure that any restrictions are transparent, justified, and minimal in impact to maintain uninterrupted access.
  - Promote digital literacy to maximize the effective use of these platforms.

Ad Hoc Policy Making:

- **Importance**: Consistent and well-thought-out policies are essential for fostering a stable digital environment. Ad hoc or reactionary policymaking creates uncertainty and can have wide-ranging negative effects.

- **Challenges**: Policies that are frequently changed or implemented without proper consultation can lead to unpredictability, making it difficult for businesses and individuals to plan and operate effectively.
- **Recommendations**:
  - Establish a collaborative policy-making process that includes stakeholders from the public and private sectors.
  - Conduct impact assessments before implementing new policies to understand their potential effects.
  - Develop long-term strategies that provide a clear direction for digital development and regulation.

Dynamic Legal Environment:

- **Importance**: Staying updated with the latest legal frameworks is crucial for ensuring compliance and leveraging digital opportunities. Laws that are clearly communicated and consistently enforced help build trust and encourage investment.
- **Challenges**: Rapid changes in laws and inconsistent enforcement can create confusion and hinder effective adaptation to new regulations.
- **Recommendations**:
  - Create accessible resources that explain legal changes and their practical implications.
  - Provide regular training and updates for businesses and public entities on new regulations.
  - Foster a culture of transparency and consistency in the enforcement of digital laws.

Revising Digital Policies:

- **Importance**: Regularly updating digital policies ensures they remain relevant and effective in addressing new technologies, practices, and workforce dynamics. This adaptability is key to maintaining efficiency and compliance.
- **Challenges**: Outdated policies can become ineffective or counterproductive, leading to inefficiencies and potential legal issues.
- **Recommendations**:
  - Establish a review cycle for digital policies to ensure they are periodically assessed and updated.
  - Involve cross-functional teams in the policy revision process to capture diverse perspectives and needs.
  - Monitor technological trends and legal changes to proactively update policies accordingly.

Modernizing Public Service Delivery:

- **Importance**: Utilizing modern digital tools and communication methods enhances the efficiency, accessibility, and transparency of public services. This can improve citizen engagement and satisfaction with public services.
- **Challenges**: Resistance to change, lack of digital infrastructure, and limited digital literacy can hinder the adoption of modernized public service delivery.
- **Recommendations**:
  - Invest in digital infrastructure to support the deployment of advanced public service platforms.

- Implement training programs for public service employees to enhance their digital skills.
- Encourage the adoption of e-government services and provide support for citizens to use these services effectively.
- Leverage data analytics to improve service delivery and decision-making processes.

References

1. National Assembly of Pakistan. (2016) *National Assembly of Pakistan Report*. Islamabad: National Assembly of Pakistan. Available at: https://www.na.gov.pk/uploads/documents/1470910659_707.pdf
2. Ministry of Information Technology and Telecommunication. (2023) *Final Draft Personal Data Protection Bill May 2023*. Islamabad: Ministry of Information Technology and Telecommunication. Available at: https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf
3. Pakistan Code. (n.d.) *Personal Data Protection Bill, 2023*. Available at: https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Noa5c%3D-sg-jjjjjjjjjjjj
4. National Response Centre for Cyber Crime. (n.d.) *Legislation*. Available at: https://www.nr3c.gov.pk/law.html
5. Council of the European Union. (n.d.) *General Data Protection Regulation (GDPR)*. Available at: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/#:~:text=The%20GDPR%20lists%20the%20rights,his%20or%20her%20personal%20data
6. IGI Global. (n.d.) *Cyber Capability Framework*. Available at: https://www.igi-global.com/dictionary/cyber-capability-framework/33101#:~:text=It%20is%20the%20mechanism%20through,the%20examples%20of%20public%20services