

CHAPTER 2

ICT POLICIES AND SAFETY ISSUES IN TEACHING AND LEARNING

This chapter presents the essential components for engaging with national ICT policies as they relate to teaching and learning. Foundational discussions introduce key terms and frameworks that enable pre-service teachers (PSTs) to understand the scope and influence of Information and Communication Technology (ICT) policies within educational settings. Building on this, policy implementation explores how these national directives shape instructional practices, guiding educators in making positive decisions that enhance pedagogy, equity, and accountability. The integration of ICT policies into learning design emphasizes how policies can be embedded in lesson planning and classroom activities, ensuring coherence between instructional intent and policy objectives. These elements form a unified framework that supports PSTs in moving from policy awareness to instructional application, preparing them to design and implement tech-enhanced learning environments that are pedagogically sound, contextually relevant, and compliant with national standards.

LESSON 1

NATIONAL OR INTERNATIONAL ICT POLICIES INTRODUCTION

National ICT policies serve as foundational guides for utilising and integrating technology into classroom instruction. These policies - such as the Department of Education's ICT in Education Masterplan, the National Framework Plan for ICTs in Basic Education, and the Digital Rise Program - outline strategic directions for equitable access, teacher capacity-building, and responsible technology use in schools. They also intersect with broader legislative frameworks like the Cybercrime Prevention Act (RA 10175), Data Privacy Act (RA 10173), and Safe Spaces Act (RA 11313), which safeguard learners and educators in digital spaces. Understanding these policies enables pre-service teachers to align their instructional decisions with national standards, ensuring that technology use in the classroom is purposeful, inclusive, and pedagogically sound. By enumerating these policies, PSTs gain clarity on the expectations and responsibilities that come with ICT integration—preparing them to become informed, policy-aware educators in a rapidly evolving educational landscape.

PRESENTATION

NATIONAL ICT POLICIES IN THE PHILIPPINES

1. DepEd ICT in Education Masterplan (2020–2025)

The DepEd ICT in Education Masterplan serves as a strategic blueprint to integrate technology into Philippine basic education. It focuses on three pillars:

- **Digital Infrastructure:** Enhancing connectivity and access to devices through the DepEd Computerization Program (DCP), including laptops, smart TVs, and

broadband installations for schools and teachers.

- **Teacher Capacity-Building:** Empowering educators via ICTS-EdTech training programs, professional development platforms (e.g., PD-LMS), and Open Educational Resources (OERs).
- **Inclusive Access:** Bridging the digital divide, especially in Last Mile Schools, through mobile learning carts, offline content, and partnerships with tech providers like Microsoft and Google.

2. National Framework Plan for ICTs in Basic Education (2005–2010)

This foundational policy, developed by DepEd and FIT-ED, laid the groundwork for ICT integration in Philippine education. Its key goals included:

- **ICT as a Tool for Quality Education:** Promoting higher-order thinking, lifelong learning, and administrative efficiency.
- **Access and Equity:** Addressing resource gaps through alternative learning systems and community-based ICT initiatives.
- **Strategic Planning:** Encouraging multi-stakeholder collaboration and evidence-based policy development.

3. Digital Rise Program

The Digital Rise Program is DepEd's flagship initiative for digital transformation. It encompasses:

- **Digital Literacy:** Embedding ICT skills in the K–12 curriculum (e.g., productivity tools, programming, multimedia).
- **ICT-Assisted Teaching:** Equipping teachers with laptops, e-learning resources, and classroom technologies.
- **ICT-Assisted Learning:** Providing learners with tablets and access to offline/online content via the DepEd LMS and DepEd Commons.

4. Cybercrime Prevention Act (RA 10175) Enacted in 2012, this law safeguards learners and educators from online threats. It criminalizes:

- **Illegal Access and Interception**
- **Cyberbullying and Online Harassment**
- **Child Pornography and Cybersex**
- **Identity Theft and Fraud**

5. Data Privacy Act (RA 10173)

This act ensures ethical and secure handling of personal data in digital learning environments. Key provisions include:

- **Consent and Transparency:** Data subjects must be informed and give consent.
- **Security Measures:** Institutions must protect data from unauthorized access or breaches.
- **Rights of Data Subjects:** Includes access, correction, erasure, and objection to processing.

6. Safe Spaces Act (RA 11313)

Also known as the Bawal Bastos Law, this act promotes respectful and safe interactions in physical and digital spaces. It addresses:

- Gender-Based Online Harassment: Including cyberstalking, sexual remarks, and non- consensual sharing of images.
- Institutional Responsibilities: Schools must implement anti-harassment policies and reporting mechanisms.
- Inclusive Protection: Covers all genders and sexual orientations. INTERNATIONAL ICT POLICY REFERENCES

1. UNESCO ICT Competency Framework for Teachers (ICT-CFT)

The UNESCO ICT-CFT Version 3 is a globally recognized framework designed to guide pre- service and in-service teacher development in integrating ICT into teaching and learning. It supports national and institutional goals by aligning teacher competencies with digital transformation priorities.

- Three Levels of Competency:
- Knowledge Acquisition: Basic ICT skills and understanding of policy.
- Knowledge Deepening: Applying ICT to enhance subject teaching and assessment.
- Knowledge Creation: Innovating pedagogical practices and contributing to digital learning environments.
- Six Core Areas:
- Understanding ICT in education
- Curriculum and assessment
- Pedagogy
- Application of digital skills
- Organization and administration
- Teacher professional learning
- 18 Competencies and 64 Objectives: These guide teacher training programs, curriculum design, and policy development.
- OER Integration: UNESCO promotes the use of Open Educational Resources (OER) aligned with ICT-CFT to support scalable, contextualized teacher training. The framework has been contextualized in various countries, including the Philippines, to support digital literacy, inclusive education, and professional development aligned with Education 2030 goals.

2. Global Education Monitoring Report (UNESCO, 2023)

The 2023 GEM Report, titled *Technology in Education: A Tool on Whose Terms?*, critically examines the role of digital technologies in education through the lenses of equity, relevance, scalability, and sustainability. ♦ Equity and Access:

- Technology can widen gaps if not equitably distributed.
- Marginalized learners often lack access to devices, connectivity, and digital content.
- Governments must ensure inclusive digital policies and infrastructure. ♦ Human-Centered Approach:

- Technology should complement, not replace, teacher-student interaction.
- Emphasis on pedagogical relevance and learner well-being. ♦ Evidence-Based Implementation:
- There are calls for rigorous evaluation of EdTech tools before adoption.
- Warns against over-reliance on private sector-driven solutions. ♦ Policy Recommendations:
- Prioritize learner needs, teacher support, and contextual appropriateness.
- Strengthen data governance, digital literacy, and regulatory frameworks.

3. OECD Digital Education Outlook (2023)

The OECD Digital Education Outlook 2023 provides a comparative analysis of how countries are shaping their digital education ecosystems, with a focus on policy trends, governance, and innovation. ♦ Digital Ecosystem Components:

- System-level tools: Student Information Systems (SIS), Education Management Information Systems (EMIS).
- Teaching and Learning Tools: LMS, digital assessments, AI-powered platforms.
- Human Component: Teacher digital competencies and professional development. ♦ AI and Emerging Technologies:
- Explores the role of AI, blockchain, and robotics in education.
- Highlights ethical considerations, data privacy, and teacher agency. ♦ Governance and Infrastructure:
- Emphasizes the need for coherent digital strategies, interoperable systems, and inclusive access.
- Encourages collaboration between governments, educators, and tech developers. ♦ Policy Recommendations:
- Develop trustworthy, effective, and equitable digital ecosystems.
- Invest in teacher capacity, infrastructure, and research-based innovation. LESSON 2 SAFETY ISSUES IN ICT INTRODUCTION Ensuring safety in the use of Information and Communication Technology (ICT) has become a critical concern for educators and learners alike. Safety issues in ICT encompass a wide range of risks from exposure to inappropriate content and cyberbullying to data privacy breaches and physical health hazards caused by prolonged device use. These concerns are not limited to technical failures but extend to ethical, legal, and behavioral dimensions of digital engagement.

In the Philippine context, national laws such as the Cybercrime Prevention Act (RA 10175) and the Data Privacy Act (RA 10173) provide legal safeguards against online threats and misuse of personal information. Globally, frameworks like UNESCO's e-Safety Guidelines and the OECD Digital Education Outlook emphasize the importance of digital citizenship, responsible technology use, and institutional policies that promote safe learning

environments. Understanding these safety issues equips pre-service teachers to foster secure, inclusive, and ethically sound ICT practices in the classroom. By recognizing potential risks and applying preventive strategies—such as ergonomic setups, password protocols, and respectful online behavior—educators can create tech-enhanced learning spaces that prioritize both innovation and well-being.

PRESENTATION

DEFINITION AND SCOPE OF ICT SAFETY

ICT Safety refers to the practices, policies, and technologies that protect individuals and organizations from harm, whether physical, psychological, or digital, arising from the use of information and communication technologies. It encompasses a broad spectrum of concerns, including cybersecurity, data privacy, online behavior, and ergonomic health.

1. Cybersecurity Threats

Cybersecurity threats involve malicious activities that compromise the integrity, confidentiality, or availability of digital systems and data. Common threats include: ♦ **Malware:** Software designed to disrupt, damage, or gain unauthorized access to systems (e.g., ransomware, spyware). Malwarebytes. (2026). Malware. <https://www.malwarebytes.com/malware> ♦ **Phishing:** Fraudulent attempts to obtain sensitive information by impersonating trustworthy entities.

Alexandra, S. (2022, October 4). What is phishing and how to prevent it. GlobalSign. <https://www.globalsign.com/en/blog/what-is-phishing> ♦ **Denial-of-Service (DoS) Attacks:** Overloading systems to make services unavailable. GeeksforGeeks. (2025, July 12). What is DDoS(Distributed Denial of Service)? <https://www.geeksforgeeks.org/computer-networks/what-is-ddos-distributed-denial-of-service/> ♦ **Zero-day Exploits:** Attacks targeting vulnerabilities before developers can patch them. Buxton, O. (2024, November 29). What is a zero-day exploit? Definition and prevention tips. Norton. <https://us.norton.com/blog/emerging-threats/zero-day-exploit>

2. Data Privacy Breaches

Shepard, S. (2018, July 17). The average cost of a data breach. Security Today. <https://securitytoday.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx> Data privacy breaches occur when personal or sensitive information is accessed, disclosed, or used without authorization. This includes:

- Unauthorized access to databases
- Improper data sharing or storage
- Identity theft and fraud In the Philippines, breaches such as the 2016 COMELEC leak exposed millions of voter records, highlighting the need for robust compliance with the Data Privacy Act of 2012 (RA 10173). Breaches can result in psychological harm, financial loss, and erosion of trust.

3. Cyberbullying and Online Harassment

Securly. (2025, July). The 10 types of cyberbullying. <https://blog.securly.com/the-10-types-of-cyberbullying/> Cyberbullying involves repeated hostile behavior via digital platforms intended to harm or intimidate others. Forms include:

- **Flaming:** Posting aggressive or insulting messages
- **Doxxing:** Publishing private information without consent
- **Cyberstalking:** Persistent online surveillance or threats

Legal protections in the Philippines include RA 10175 (Cybercrime Prevention Act) and RA 10627 (Anti-Bullying Act), which mandate schools and institutions to address digital harassment. Victims may suffer emotional distress, academic decline, and mental health issues.

4. Ergonomic and Health Risks

Fogel, R. (2020, May 8). The health risks of a poor ergonomic workspace. Accredited Rehabilitation Consultants.

<https://ergoevaluation.com/the-health-risks-of-a-poor-ergonomic-workspace/> Prolonged ICT use can lead to physical and psychological health concerns, such as:

- **Repetitive Strain Injuries (RSI):** Caused by repetitive keyboard/mouse use
- **Eye Strain:** Resulting from extended screen exposure
- **Poor Posture:** Leading to musculoskeletal disorders
- **Sleep Disruption:** Due to excessive screen time
Ergonomic hazards are often overlooked but can significantly affect productivity and well-being. Best practices include proper workstation setup, regular breaks, and screen time management.