

การบริหารเครือข่ายสถานศึกษาเพื่อเสริมสร้างภูมิคุ้มกันภัยออนไลน์ในยุคดิจิทัล
SCHOOL NETWORK ADMINISTRATION TO ENHANCE ONLINE SAFETY
IMMUNITY IN THE DIGITAL ERA

กชกร หนูพวง¹, ฐิติมา ธรรมเรียง² และอรวรรณ สิงห์ชู³

Kotchakorn Noopuang¹, Thitima Thamriang² and Orawan Singchoo³

มหาวิทยาลัยราชภัฏสุราษฎร์ธานี

Suratthani Rajabhat University

68052503007@student.sru.ac.th



บทคัดย่อ

การเปลี่ยนผ่านสู่สังคมดิจิทัลได้ส่งผลกระทบต่อระบบการศึกษาอย่างลึกซึ้ง ทั้งในด้านรูปแบบการจัดการเรียนรู้ การบริหารสถานศึกษา และพฤติกรรมการใช้เทคโนโลยีของผู้เรียน เทคโนโลยีดิจิทัลได้เปิดโอกาสในการเข้าถึงองค์ความรู้และพัฒนาศักยภาพการเรียนรู้ หากแต่การขยายตัวของสภาพแวดล้อมทางโลกออนไลน์ ได้นำมาซึ่งความเสี่ยงด้านความปลอดภัยไซเบอร์ การละเมิดข้อมูลส่วนบุคคล การกลั่นแกล้งออนไลน์ และภัยคุกคามเชิงสังคม เทคนิคที่ส่งผลกระทบต่อผู้เรียน ครู และองค์กรทางการศึกษาในภาพรวม ความท้าทายดังกล่าวสะท้อนให้เห็นว่าการพัฒนาทักษะดิจิทัลเพียงอย่างเดียวไม่เพียงพอ หากต้องควบคู่กับการเสริมสร้างภูมิคุ้มกันทางดิจิทัล และการบริหารจัดการเชิงระบบ

บทความวิชาการนี้มุ่งวิเคราะห์บริบทภัยออนไลน์ในระบบการศึกษาไทย สังเคราะห์แนวคิดการบริหารเครือข่ายสถานศึกษา และบูรณาการกรอบความเป็นพลเมืองดิจิทัลกับหลักการความปลอดภัยไซเบอร์ เพื่อนำไปสู่การพัฒนาแนวคิดการบริหารเครือข่ายเพื่อเสริมสร้างภูมิคุ้มกันภัยออนไลน์อย่างเป็นองค์รวม การศึกษาดำเนินการโดยใช้การทบทวนวรรณกรรมเชิงวิเคราะห์จากงานวิจัย หนังสือวิชาการ รายงานขององค์การระหว่างประเทศ และเอกสารเชิงนโยบาย เพื่อนำมาสังเคราะห์เป็นกรอบแนวคิดเชิงบูรณาการ

ผลการสังเคราะห์ชี้ให้เห็นว่า การเสริมสร้างความปลอดภัยดิจิทัลในสถานศึกษาจำเป็นต้องอาศัยความร่วมมือของหลายภาคส่วน การพัฒนาพลเมืองดิจิทัลของผู้เรียนและบุคลากร การจัดให้มีระบบเฝ้าระวังและกลไกป้องกันภัยไซเบอร์ ตลอดจนการสนับสนุนเชิงนโยบายและการบริหารเชิงยุทธศาสตร์ในระดับชาติ และระดับสถานศึกษาอย่างสอดคล้องกัน บทความนี้จึงเสนอกรอบการบริหารเครือข่ายที่เชื่อมโยงมิติทางเทคโนโลยี สังคม และนโยบายเข้าไว้ด้วยกัน เพื่อสนับสนุนการพัฒนาระบบการศึกษาที่ปลอดภัย ยืดหยุ่น และยั่งยืนในบริบทของสังคมดิจิทัล

คำสำคัญ : การบริหารเครือข่ายสถานศึกษา , ความปลอดภัยดิจิทัล , ภัยออนไลน์ , การบริหารการศึกษา

*Received February 25, 2026; Revised March 20, 2026; Accepted April 5, 2026

Abstract

The transition toward a digital society has profoundly transformed educational systems in terms of learning management approaches, school administration, and students' patterns of technology use. Digital technologies have created new opportunities for accessing knowledge and enhancing learning potential. However, the rapid expansion of online environments has also introduced significant risks, including cybersecurity threats, data privacy violations, cyberbullying, and broader socio-technical challenges that affect students, teachers, and educational institutions as a whole. These challenges indicate that the development of digital skills alone is insufficient; it must be accompanied by the strengthening of digital resilience and systematic governance mechanisms.

This academic article aims to analyze the context of online risks within the Thai educational system, synthesize concepts of network governance in educational institutions, and integrate the frameworks of digital citizenship and cybersecurity principles in order to propose a holistic model of network-based management for enhancing online risk resilience. The study employs an analytical literature review of research articles, academic books, international organizational reports, and policy documents to develop an integrated conceptual framework.

The findings suggest that strengthening digital safety in educational institutions requires multi-sector collaboration, the development of digital citizenship competencies among students and personnel, the establishment of proactive monitoring systems and cybersecurity protection mechanisms, and coherent policy support and strategic governance at both national and institutional levels. The article proposes an integrated network governance framework that connects technological, social, and policy dimensions to support the development of a safe, adaptive, and sustainable education system in the digital era.

Keywords : Educational network governance , Digital safety , Online risks ,
Educational administration

บทนำ

การพัฒนาเทคโนโลยีดิจิทัลในศตวรรษที่ 21 ได้ส่งผลให้ระบบการศึกษาทั่วโลก เกิดการเปลี่ยนแปลงอย่างเห็นได้ชัด ทั้งในด้านกระบวนการเรียนรู้ การบริหารจัดการศึกษา และรูปแบบปฏิสัมพันธ์ ระหว่างผู้เรียนกับสภาพแวดล้อมการเรียนรู้ เทคโนโลยีสารสนเทศ แพลตฟอร์มการเรียนรู้ออนไลน์ สื่อสังคมดิจิทัล และระบบเครือข่ายอินเทอร์เน็ตความเร็วสูง ได้กลายเป็นองค์ประกอบสำคัญของการจัดการศึกษายุคใหม่ โดยเฉพาะหลังสถานการณ์การแพร่ระบาดของ COVID-19 ที่ผลักดันให้สถานศึกษา ต้องปรับรูปแบบการเรียนการสอนสู่ระบบออนไลน์อย่างรวดเร็ว ส่งผลให้ผู้เรียนมีการใช้งานเทคโนโลยีดิจิทัล ในชีวิตประจำวันเพิ่มขึ้นอย่างมีนัยสำคัญ ทั้งเพื่อการศึกษา การสื่อสาร และการสร้างเครือข่ายสังคมออนไลน์ การขยายตัวของเทคโนโลยีดิจิทัลดังกล่าว ได้นำมาซึ่งความเสี่ยง ด้านความปลอดภัยไซเบอร์ ในหลายมิติ เช่น การกลั่นแกล้งทางออนไลน์ (cyberbullying) การละเมิดข้อมูลส่วนบุคคล การใช้กลอุบายหลอกลวงผ่านเครือข่ายอินเทอร์เน็ต การเข้าถึงเนื้อหาที่ไม่เหมาะสม รวมถึงความเสี่ยงด้านสุขภาวะจิต จากการใช้สื่อดิจิทัลอย่างไม่เหมาะสม ปัญหาเหล่านี้ส่งผลกระทบ ต่อพัฒนาการทางอารมณ์ และพฤติกรรมของผู้เรียนอย่างต่อเนื่อง โดยเฉพาะในกลุ่มเด็กและเยาวชนที่ยังขาดทักษะการรู้เท่าทันสื่อ และการป้องกันตนเองในโลกดิจิทัล (Livingstone et al., 2017)

ในเชิงการบริหารการศึกษา นักวิชาการจำนวนมากเสนอว่า การพัฒนาทักษะดิจิทัลของผู้เรียนเพียงด้านเทคนิค ไม่เพียงพอต่อการรับมือความเสี่ยงในโลกออนไลน์ แต่จำเป็นต้องบูรณาการการพัฒนาความตระหนักด้านจริยธรรมดิจิทัล ความรับผิดชอบต่อสังคมออนไลน์ และความปลอดภัยไซเบอร์ควบคู่กันไป การส่งเสริมแนวคิดพลเมืองดิจิทัล จึงมีความสำคัญต่อการสร้างภูมิคุ้มกัน ให้ผู้เรียนสามารถใช้เทคโนโลยีอย่างสร้างสรรค์ ปลอดภัย และมีวิจารณญาณ (Ribble, 2015) นอกจากนี้ แนวคิดการบริหารเครือข่ายองค์กรในยุคสังคมดิจิทัลชี้ให้เห็นว่าการแก้ไขปัญหาที่มีความซับซ้อน เช่น ความปลอดภัยไซเบอร์ของผู้เรียน ไม่สามารถดำเนินการโดยสถานศึกษาเพียงลำพัง แต่ต้องอาศัยความร่วมมือระหว่างหลายภาคส่วน ได้แก่ หน่วยงานภาครัฐ ภาคเอกชน ชุมชน ผู้ปกครอง และองค์กรด้านเทคโนโลยีสารสนเทศ การบริหารเครือข่ายเชิงความร่วมมือ จึงเป็นกลไกสำคัญในการแลกเปลี่ยนข้อมูล ความรู้ ทรัพยากร และมาตรการป้องกันภัยออนไลน์อย่างเป็นระบบ ซึ่งสอดคล้องกับแนวคิดสังคมเครือข่ายที่เน้นบทบาทของการเชื่อมโยงข้อมูล และความร่วมมือข้ามองค์กรในการแก้ปัญหาสังคมร่วมสมัย (Castells, 2010) ด้วยเหตุนี้ การบริหารเครือข่ายสถานศึกษาเพื่อเสริมสร้างภูมิคุ้มกันภัยออนไลน์ จึงเป็นประเด็นสำคัญ ทางวิชาการและเชิงนโยบาย ในยุคดิจิทัล บทความนี้จึงมุ่งนำเสนอการวิเคราะห์ เกี่ยวกับบริบทภัยออนไลน์ในระบบการศึกษา แนวคิดการบริหารเครือข่ายสถานศึกษา การพัฒนาพลเมืองดิจิทัล และแนวทางเชิงระบบในการสร้างความปลอดภัยไซเบอร์ เพื่อสนับสนุนการพัฒนาการศึกษาที่มีคุณภาพ ปลอดภัย และยั่งยืนในศตวรรษที่ 21

เนื้อหา

แนวคิดการบริหารเครือข่ายสถานศึกษา

แนวคิดการบริหารเครือข่ายเกิดขึ้นจากการเปลี่ยนแปลงของรูปแบบองค์กรในยุคโลกาภิวัตน์ และสังคมดิจิทัล ซึ่งองค์กรไม่สามารถดำเนินงานแบบแยกส่วน หรือใช้โครงสร้างแบบลำดับชั้นเพียงอย่างเดียว แต่จำเป็นต้องอาศัยการประสานความร่วมมือ การแลกเปลี่ยนทรัพยากร และการสร้างความสัมพันธ์ระหว่างองค์กรเพื่อเพิ่มขีดความสามารถในการแข่งขัน และประสิทธิภาพการดำเนินงาน (Castells, 2010; Provan & Kenis, 2008) ทั้งนี้ Putnam (2000) ได้อธิบายว่าเครือข่ายทางสังคมมีบทบาทสำคัญในการสร้างทุนทางสังคม

ซึ่งส่งผลต่อระดับความไว้วางใจ ความร่วมมือและประสิทธิผลขององค์กร โดยเฉพาะองค์กรที่ต้องเผชิญกับการเปลี่ยนแปลงทางสังคม และเทคโนโลยีอย่างรวดเร็ว

ในบริบททางการศึกษา แนวคิดเครือข่ายสถานศึกษาได้รับการนำมาใช้เพื่อส่งเสริมความร่วมมือระหว่างโรงเรียน หน่วยงานภาครัฐ ชุมชน ผู้ปกครอง สถาบันอุดมศึกษา และภาคเอกชน เพื่อพัฒนาคุณภาพการจัดการศึกษาอย่างรอบด้าน ทั้งในมิติการเรียนรู้ของผู้เรียน การพัฒนาวิชาชีพครู การบริหารทรัพยากรทางการศึกษา และการสร้างนวัตกรรมทางการศึกษา (Hargreaves & Fullan, 2012) เครือข่ายสถานศึกษาจึงมิได้เป็นเพียงความร่วมมือเชิงกิจกรรม แต่เป็นระบบความสัมพันธ์เชิงโครงสร้างที่ช่วยเสริมสร้างศักยภาพองค์กรการศึกษาให้สามารถปรับตัวต่อการเปลี่ยนแปลงของสังคมดิจิทัลได้อย่างมีประสิทธิภาพ

การบริหารเครือข่ายสถานศึกษาประกอบด้วยองค์ประกอบสำคัญหลายประการ ได้แก่ ภาวะผู้นำเชิงเครือข่ายที่เน้นการสร้างวิสัยทัศน์ร่วม และการประสานความร่วมมือ ระบบการสื่อสารและสารสนเทศเพื่อสนับสนุนการตัดสินใจเชิงนโยบาย การแลกเปลี่ยนทรัพยากรทั้งด้านบุคลากร ความรู้ เทคโนโลยี และงบประมาณ ตลอดจน กลไกการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียจากหลายภาคส่วน Bryman (2012) ชี้ให้เห็นว่า การมีส่วนร่วมเชิงเครือข่าย ช่วยเพิ่มความโปร่งใส ความไว้วางใจ และประสิทธิภาพการดำเนินงานขององค์กร ซึ่งในบริบทการศึกษาจะส่งผลต่อคุณภาพการจัดการเรียนรู้ และการพัฒนาผู้เรียนโดยตรง ด้านการสร้างเครือข่ายความร่วมมือระหว่างสถานศึกษา สามารถส่งเสริมการแลกเปลี่ยนองค์ความรู้ทางวิชาชีพครู การพัฒนาหลักสูตรร่วม การจัดกิจกรรมการเรียนรู้ข้ามโรงเรียน และการใช้ทรัพยากรทางการศึกษาร่วมกัน ซึ่งส่งผลให้เกิดประสิทธิภาพการบริหารจัดการที่สูงขึ้น (Muijs et al., 2011) นอกจากนี้ เครือข่ายสถานศึกษา ยังมีบทบาทสำคัญในการแก้ไขปัญหาสังคมที่ส่งผลต่อโรงเรียน เช่น ความเหลื่อมล้ำทางการศึกษา ปัญหาพฤติกรรมเสี่ยงของผู้เรียน และความปลอดภัยในโลกออนไลน์ โดยอาศัยความร่วมมือจากหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้าน ซึ่งในยุคดิจิทัลเทคโนโลยีสารสนเทศ และการสื่อสารมีบทบาทสำคัญต่อการบริหารเครือข่ายสถานศึกษา อย่างหลีกเลี่ยงไม่ได้ ระบบฐานข้อมูลออนไลน์ ระบบบริหารจัดการเรียนรู้ แพลตฟอร์มการประชุมทางไกล และเครือข่ายสื่อสังคมดิจิทัล ช่วยให้การประสานงานระหว่างหน่วยงานเกิดขึ้นอย่างรวดเร็ว โปร่งใส และมีประสิทธิภาพมากขึ้น อีกทั้งยังสนับสนุนการติดตามและประเมินผลการดำเนินงานของเครือข่ายได้อย่างเป็นระบบ Selwyn (2016) ชี้ให้เห็นว่า เทคโนโลยีดิจิทัล ไม่เพียงแต่เป็นเครื่องมือสนับสนุนการเรียนรู้เท่านั้น แต่ยังเป็นกลไกสำคัญในการบริหารองค์กรการศึกษา และการสร้างเครือข่ายความร่วมมือในระดับท้องถิ่น ระดับประเทศ และระดับนานาชาติ

นอกจากนี้ เทคโนโลยีดิจิทัลยังมีบทบาทในการเฝ้าระวัง และป้องกันภัยออนไลน์ในสถานศึกษา เช่น ระบบติดตามพฤติกรรมการใช้อินเทอร์เน็ตของผู้เรียน ระบบแจ้งเตือนภัยไซเบอร์ และการให้ความรู้ด้านความปลอดภัยดิจิทัลผ่านแพลตฟอร์มออนไลน์ การบูรณาการเทคโนโลยีกับการบริหารเครือข่ายจึงช่วยเพิ่มประสิทธิภาพการดูแลผู้เรียนทั้งด้านวิชาการ สังคม และความปลอดภัยไซเบอร์อย่างครอบคลุม (UNESCO, 2019) ดังนั้นการบริหารเครือข่ายสถานศึกษาในยุคดิจิทัลควรเน้นการบูรณาการความร่วมมือหลายภาคส่วน การใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการสื่อสารและการตัดสินใจเชิงนโยบาย การพัฒนาศักยภาพบุคลากรด้านดิจิทัล และการสร้างระบบสนับสนุนความปลอดภัยไซเบอร์อย่างยั่งยืน ซึ่งจะช่วยให้สถานศึกษาสามารถตอบสนองต่อความท้าทายของการศึกษาในศตวรรษที่ 21 ได้อย่างมีประสิทธิภาพ

ความเป็นพลเมืองดิจิทัล

แนวคิดความเป็นพลเมืองดิจิทัล (digital citizenship) ได้รับความสนใจอย่างกว้างขวางในแวดวงการศึกษาในช่วงทศวรรษที่ผ่านมา เนื่องจากการขยายตัวของเทคโนโลยีสารสนเทศ และการสื่อสารได้เปลี่ยนแปลงรูปแบบการเรียนรู้ และการดำรงชีวิตของผู้เรียนอย่างรวดเร็ว ผู้เรียนในศตวรรษที่ 21 จำเป็นต้องดำรงชีวิตอยู่ในสภาพแวดล้อมดิจิทัลอย่างหลีกเลี่ยงไม่ได้ ส่งผลให้แนวคิดพลเมืองดิจิทัลถูกนำมาใช้เป็นกรอบในการพัฒนาคุณลักษณะของผู้เรียนให้สามารถใช้เทคโนโลยีได้อย่างมีความรับผิดชอบ มีจริยธรรมปลอดภัย และสร้างสรรค์ โดย Ribble (2015) ให้ความหมายว่า พลเมืองดิจิทัล หมายถึง ความสามารถของบุคคลในการใช้เทคโนโลยีดิจิทัลอย่างเหมาะสม โดยครอบคลุมด้านความรู้ ทักษะ เจตคติ และคุณลักษณะทางจริยธรรมที่เกี่ยวข้องกับการใช้สื่อดิจิทัล แนวคิดดังกล่าวนี้ได้จำกัดเฉพาะทักษะทางเทคนิคเท่านั้น แต่ยังรวมถึงความสามารถในการคิดเชิงวิพากษ์ การตระหนักรู้ถึงผลกระทบของเทคโนโลยีต่อสังคม และความรับผิดชอบต่อการกระทำของตนในโลกออนไลน์ (UNESCO, 2019) ซึ่งองค์ประกอบสำคัญของความเป็นพลเมืองดิจิทัลประกอบด้วยหลายมิติ ได้แก่ การรู้เท่าทันสื่อและสารสนเทศ ความปลอดภัย และความมั่นคงทางดิจิทัล จริยธรรมดิจิทัล การสื่อสารอย่างรับผิดชอบในสังคมออนไลน์ ตลอดจนความเข้าใจด้านสิทธิและหน้าที่ของผู้ใช้เทคโนโลยี การพัฒนาทักษะเหล่านี้ช่วยให้ผู้เรียนสามารถประเมินข้อมูลอย่างมีวิจารณญาณ ป้องกันตนเองจากภัยออนไลน์ มีส่วนร่วมในสังคมดิจิทัลอย่างสร้างสรรค์ และมีความรับผิดชอบ (Hollandsworth, Dowdy, and Donovan, 2011)

หากพิจารณา ตาม Floridi (2014) ที่เสนอแนวคิดจริยธรรมสารสนเทศ (information ethics) ซึ่งเน้นความรับผิดชอบต่อการใช้ข้อมูลดิจิทัล โดยชี้ให้เห็นว่า การใช้ข้อมูลและเทคโนโลยีไม่ควรพิจารณาเฉพาะประสิทธิภาพหรือประโยชน์เชิงเทคนิคเท่านั้น แต่ต้องคำนึงถึงผลกระทบด้านจริยธรรม สังคม และความเป็นส่วนตัวของบุคคล แนวคิดดังกล่าวมีความสำคัญอย่างยิ่งในบริบทการศึกษา เนื่องจากผู้เรียนจำนวนมากยังขาดความตระหนักรู้เกี่ยวกับความเป็นส่วนตัว ความปลอดภัยข้อมูล และผลกระทบของการเผยแพร่ข้อมูลส่วนบุคคลในโลกออนไลน์ ขณะเดียวกันทฤษฎีการเรียนรู้ทางสังคมของ Bandura (1991) อธิบายว่าพฤติกรรมของบุคคลได้รับอิทธิพลจากการสังเกตแบบอย่างทางสังคม การเสริมแรง และสภาพแวดล้อมทางสังคม แนวคิดนี้สามารถอธิบายพฤติกรรมออนไลน์ของผู้เรียนได้อย่างชัดเจน กล่าวคือ ผู้เรียนมักเลียนแบบพฤติกรรมจากสื่อสังคมออนไลน์ เพื่อน หรือบุคคลต้นแบบ ดังนั้นการสร้างสภาพแวดล้อมดิจิทัลเชิงบวกในโรงเรียน รวมถึงการมีแบบอย่างที่ดีจากครูและผู้บริหาร จึงมีบทบาทสำคัญในการหล่อหลอมพฤติกรรมดิจิทัลของผู้เรียนให้เป็นไปในทิศทางที่เหมาะสมและปลอดภัย ในบริบทการศึกษา การส่งเสริมความเป็นพลเมืองดิจิทัลควรดำเนินการอย่างเป็นระบบ ผ่านหลักสูตรการเรียนรู้ การจัดกิจกรรมเสริมสร้างทักษะดิจิทัลและการสร้างวัฒนธรรมองค์กร ที่สนับสนุนการใช้เทคโนโลยีอย่างรับผิดชอบ การบูรณาการประเด็นพลเมืองดิจิทัลในหลักสูตร มิได้เป็นเพียงการช่วยลดความเสี่ยงด้านความปลอดภัยไซเบอร์ แต่ยังส่งเสริมทักษะสำคัญในศตวรรษที่ 21 เช่น การคิดวิเคราะห์ การสื่อสาร การทำงานร่วมกัน และการเรียนรู้ตลอดชีวิต (Partnership for 21st Century Learning, 2015)

นอกจากนี้การพัฒนาพลเมืองดิจิทัลยังมีความสัมพันธ์กับการสร้างภูมิคุ้มกันทางจิตสังคมของผู้เรียน ผู้เรียนที่มีทักษะพลเมืองดิจิทัลสูงมักสามารถจัดการความเสี่ยงออนไลน์ได้ดี มีความตระหนักรู้เกี่ยวกับผลกระทบของสื่อดิจิทัลต่อสุขภาวะ และสามารถสร้างสมดุลระหว่างชีวิตออนไลน์ และออฟไลน์ได้อย่างเหมาะสม การพัฒนาองค์ความรู้ดังกล่าวจึงมีบทบาทสำคัญต่อการพัฒนาคุณภาพชีวิต และศักยภาพการเรียนรู้ของผู้เรียนในระยะยาว (Livingstone & Smith, 2014) อีกประเด็นหนึ่งที่มีความสำคัญ คือ บทบาทของครูและผู้บริหารสถานศึกษาในการเป็นผู้นำด้านพลเมืองดิจิทัล ครูควรได้รับการพัฒนาสมรรถนะด้านดิจิทัล

และจริยธรรมสารสนเทศอย่างต่อเนื่อง เพื่อให้สามารถถ่ายทอดความรู้และเป็นแบบอย่างที่ดีแก่ผู้เรียน ขณะเดียวกัน ผู้บริหารสถานศึกษา ควรส่งเสริมการกำหนดนโยบายด้านความปลอดภัยดิจิทัล การใช้เทคโนโลยี อย่างรับผิดชอบ และการสร้างเครือข่ายความร่วมมือกับผู้ปกครองและชุมชน เพื่อสร้างระบบสนับสนุน การพัฒนา พลเมืองดิจิทัลอย่างยั่งยืน (Fullan, 2014) สะท้อนให้เห็นว่า ในภาพรวมความเป็นพลเมืองดิจิทัล มิใช่เพียงทักษะส่วนบุคคล แต่เป็นองค์ประกอบสำคัญของระบบนิเวศการศึกษาดิจิทัล (Castells, 2010) ที่ต้องอาศัยความร่วมมือระหว่างผู้เรียน ครู ผู้บริหาร ผู้ปกครอง และสังคมโดยรวม การพัฒนาพลเมืองดิจิทัล อย่างเป็นระบบจะช่วยเสริมสร้างภูมิคุ้มกันภัยออนไลน์ ลดความเสี่ยงด้านพฤติกรรมดิจิทัลที่ไม่เหมาะสม และส่งเสริมการใช้เทคโนโลยีเพื่อการพัฒนาสังคมอย่างยั่งยืน

ความปลอดภัยดิจิทัลในสถานศึกษา

ความปลอดภัยดิจิทัล (digital safety) หมายถึง กระบวนการ มาตรการ และระบบที่ใช้เพื่อป้องกัน ข้อมูล ระบบเทคโนโลยี และผู้ใช้จากภัยคุกคามทางไซเบอร์ เช่น มัลแวร์ การโจรกรรมข้อมูล การละเมิด ความเป็นส่วนตัว การหลอกลวงทางออนไลน์ และการคุกคามผ่านสื่อดิจิทัล (OECD, 2021) ในบริบทของ สถานศึกษา ความปลอดภัยดิจิทัลไม่ได้จำกัดเพียงด้านเทคนิคเท่านั้น แต่ยังครอบคลุมถึงมิติทางจิตวิทยา สังคม จริยธรรม และการบริหารจัดการองค์กร เนื่องจากผู้เรียน ครู และบุคลากรทางการศึกษาต่างเป็นผู้ใช้เทคโนโลยี ดิจิทัลอย่างต่อเนื่องในกระบวนการเรียนรู้ การสื่อสาร และการบริหารการศึกษา ความสำคัญ ของความปลอดภัยดิจิทัลในสถานศึกษาเพิ่มขึ้นอย่างต่อเนื่องตามการขยายตัวของ การเรียนรู้ออนไลน์ แพลตฟอร์มการเรียนรู้ดิจิทัล และการใช้เครือข่ายสังคมออนไลน์ในหมู่ผู้เรียน การเรียนรู้ผ่านระบบออนไลน์ ช่วยเพิ่มโอกาสทางการศึกษา แต่ขณะเดียวกันก็เพิ่มความเสี่ยง ต่อภัยคุกคามทางไซเบอร์ เช่น การรั่วไหล ของข้อมูลผู้เรียน การถูกโจมตีทางไซเบอร์ต่อระบบสถานศึกษา และการคุกคามทางออนไลน์ที่ส่งผลกระทบต่อ สุขภาวะทางจิตของผู้เรียน หากขาดมาตรการป้องกันที่เหมาะสม ปัญหาเหล่านี้อาจส่งผลกระทบต่อคุณภาพ การศึกษา ความเชื่อมั่นของผู้ปกครอง และภาพลักษณ์ของสถานศึกษา

การศึกษาของ Livingstone et al. (2017) จำแนกภัยออนไลน์ของเด็กและเยาวชนออกเป็น 4 กลุ่มหลัก ได้แก่ (1) ความเสี่ยงด้านเนื้อหา เช่น การเข้าถึงเนื้อหาที่ไม่เหมาะสมหรือเป็นอันตราย (2) ความเสี่ยง ด้านการติดต่อ เช่น การถูกล่อลวงหรือคุกคามผ่านสื่อออนไลน์ (3) ความเสี่ยงด้านพาณิชย์ เช่น การถูกหลอกลวงทางการเงินหรือการละเมิดข้อมูลส่วนบุคคล และ (4) ความเสี่ยงด้านพฤติกรรม เช่น การกลั่นแกล้งออนไลน์ หรือการใช้สื่ออย่างไม่เหมาะสม การจำแนกดังกล่าวสะท้อนให้เห็นว่า ภัยออนไลน์ มีความซับซ้อน และจำเป็นต้องใช้มาตรการป้องกันหลายระดับ ทั้งด้านเทคนิค การบริหารจัดการ และการพัฒนาทักษะผู้เรียน

ในเชิงเทคนิค ความปลอดภัยดิจิทัลในสถานศึกษา ควรครอบคลุมการป้องกันระบบเครือข่าย การจัดการข้อมูล และการควบคุมการเข้าถึงข้อมูล เช่น การใช้ระบบ firewall การเข้ารหัสข้อมูล ระบบตรวจจับการบุกรุก และมาตรการสำรองข้อมูลอย่างสม่ำเสมอ นอกจากนี้ การจัดทำนโยบาย ความปลอดภัยข้อมูล (information security policy) ที่ชัดเจนจะช่วยลด ความเสี่ยงด้านการบริหารจัดการ และสร้างมาตรฐานการปฏิบัติที่เหมาะสมสำหรับบุคลากร และผู้เรียน ในด้านการศึกษา การสร้าง ความปลอดภัยดิจิทัลต้องอาศัยการพัฒนาความรู้ร่วมกับทักษะของผู้เรียน ครู และบุคลากรทางการศึกษา เกี่ยวกับการใช้เทคโนโลยีอย่างปลอดภัย อีกทั้งด้านการรู้เท่าทันสื่อ การป้องกันข้อมูลส่วนบุคคล และการรับมือ กับภัยออนไลน์ การให้ความรู้ ด้านความปลอดภัยไซเบอร์ ควรบูรณาการในหลักสูตรการเรียนรู้ กิจกรรม เสริมหลักสูตร และการพัฒนาวิชาชีพครูอย่างต่อเนื่อง อีกประการหนึ่งที่สำคัญ คือ บทบาทของวัฒนธรรม

องค์กรในการส่งเสริมความปลอดภัยดิจิทัล สถานศึกษาควรสร้างบรรยากาศที่ส่งเสริมการใช้เทคโนโลยีอย่างรับผิดชอบ การเคารพสิทธิของผู้อื่น และการตระหนักถึงผลกระทบของการกระทำออนไลน์ การสร้างวัฒนธรรมดังกล่าว ช่วยลดพฤติกรรมเสี่ยง และส่งเสริมการใช้เทคโนโลยีเพื่อการเรียนรู้อย่างสร้างสรรค์

ในระดับนโยบาย การบริหารความปลอดภัยดิจิทัลจำเป็นต้องได้รับการสนับสนุน จากหน่วยงานต้นสังกัด และภาครัฐ ผ่านการกำหนดมาตรฐานความปลอดภัยไซเบอร์ การพัฒนาระบบโครงสร้างพื้นฐานดิจิทัล และการสนับสนุนงบประมาณ สำหรับการพัฒนาเทคโนโลยีและการฝึกอบรมบุคลากร นโยบายระดับชาติมีบทบาทสำคัญในการกำหนดทิศทางการพัฒนาความปลอดภัยดิจิทัลในระบบการศึกษาอย่างยั่งยืน นอกจากนี้ ความร่วมมือระหว่างสถานศึกษา ผู้ปกครอง ชุมชน และภาคเอกชน ยังเป็นปัจจัยสำคัญในการเสริมสร้างความปลอดภัยดิจิทัล เครือข่ายความร่วมมือช่วยให้เกิดการแลกเปลี่ยนข้อมูล เกี่ยวกับภัยออนไลน์ การพัฒนามาตรการป้องกันร่วมกัน และการสนับสนุนทรัพยากรด้านเทคโนโลยี ความรู้ ความร่วมมือดังกล่าว มีความสำคัญอย่างยิ่งในยุคดิจิทัลที่ภัยไซเบอร์มีลักษณะข้ามพรมแดน (OECD, 2021) และเปลี่ยนแปลงอย่างรวดเร็ว เมื่อพิจารณาในภาพรวม ความปลอดภัยดิจิทัลในสถานศึกษาจึงเป็นประเด็นที่ต้องพิจารณาแบบองค์รวม ครอบคลุมทั้งด้านเทคนิค การบริหารจัดการ การพัฒนาทักษะผู้เรียน วัฒนธรรมองค์กร และนโยบายระดับชาติ การบูรณาการองค์ประกอบเหล่านี้จะช่วยสร้างระบบนิเวศการเรียนรู้ที่ปลอดภัย ลดความเสี่ยงจากภัยไซเบอร์ และส่งเสริมการใช้เทคโนโลยีเพื่อการพัฒนาการศึกษาอย่างยั่งยืน

รูปแบบการบริหารเครือข่ายเพื่อเสริมสร้างภูมิคุ้มกันภัยออนไลน์

จากการสังเคราะห์แนวคิด ทฤษฎี สามารถเสนอรูปแบบการบริหาร เครือข่ายสถานศึกษา เพื่อเสริมสร้างภูมิคุ้มกันภัยออนไลน์ของผู้เรียน ครู และบุคลากรทางการศึกษา ในยุคดิจิทัลได้อย่างเป็นระบบ โดยมุ่งเน้นการบูรณาการความร่วมมือหลายภาคส่วน การพัฒนาทักษะพลเมืองดิจิทัล การเสริมสร้างระบบความปลอดภัยไซเบอร์ และการกำหนดนโยบายเชิงระบบในระดับสถานศึกษา และระดับประเทศ รูปแบบดังกล่าวตั้งอยู่บนหลักการสำคัญคือ การบริหารแบบเครือข่าย การมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย และการใช้ข้อมูลเชิงประจักษ์ในการตัดสินใจเชิงนโยบาย แนวคิดการบริหารเครือข่ายเพื่อเสริมสร้างภูมิคุ้มกันภัยออนไลน์ มิได้จำกัดอยู่เพียงการป้องกันภัยไซเบอร์เชิงเทคนิคเท่านั้น แต่ยังครอบคลุมมิติทางสังคม จิตวิทยา วัฒนธรรม และจริยธรรมดิจิทัล ซึ่งมีผลต่อพฤติกรรมการใช้เทคโนโลยีของผู้เรียนโดยตรง การสร้างภูมิคุ้มกันจึงต้องดำเนินการทั้งในระดับบุคคล ระดับองค์กร และระดับเครือข่าย สังคมการศึกษา โดยอาศัยการบูรณาการทรัพยากร ความรู้ และความเชี่ยวชาญจากหลายภาคส่วน รูปแบบการบริหารเครือข่ายดังกล่าวสามารถจำแนกเป็น 4 มิติหลัก ดังนี้

มิติที่หนึ่ง มิติความร่วมมือเครือข่าย

ความร่วมมือเครือข่าย (Provan & Kenis, 2008) ความร่วมมือเครือข่ายถือเป็นกลไกหลักในการขับเคลื่อนการสร้างภูมิคุ้มกันภัยออนไลน์ในสถานศึกษา เนื่องจากปัญหาความปลอดภัยไซเบอร์มีลักษณะซับซ้อน และเชื่อมโยงหลายภาคส่วน การดำเนินงานโดยสถานศึกษาเพียงลำพังมักไม่เพียงพอ จึงจำเป็นต้องอาศัยความร่วมมือจากหน่วยงานรัฐ องค์กรเอกชน ผู้เชี่ยวชาญด้านเทคโนโลยี ผู้ปกครอง ชุมชน และองค์กรภาคประชาสังคม ความร่วมมือดังกล่าว สามารถดำเนินการได้หลายรูปแบบ เช่น การจัดตั้งเครือข่ายความปลอดภัย ไซเบอร์ระดับเขตพื้นที่การศึกษา การสร้างแพลตฟอร์มแลกเปลี่ยนข้อมูลข่าวสารด้านภัยออนไลน์ การจัดกิจกรรมอบรมร่วมระหว่างโรงเรียนและองค์กรเทคโนโลยี ตลอดจนการพัฒนาหลักสูตร ร่วมที่เน้นทักษะการใช้งานเทคโนโลยีอย่างปลอดภัย นอกจากนี้ การสร้างเครือข่ายยังช่วยให้เกิดการแบ่งปันทรัพยากร

ทั้งด้านองค์ความรู้ เทคโนโลยี บุคลากร และงบประมาณ ส่งผลให้สถานศึกษาที่มีข้อจำกัดด้านทรัพยากรสามารถเข้าถึงเครื่องมือและองค์ความรู้ด้านความปลอดภัยไซเบอร์ได้มากขึ้น อีกทั้งยังช่วยสร้างชุมชนแห่งการเรียนรู้ทางวิชาชีพที่ส่งเสริมการพัฒนาครู และบุคลากรทางการศึกษาอย่างต่อเนื่อง

มิติที่สอง มิติการพัฒนาพลเมืองดิจิทัล

การพัฒนาพลเมืองดิจิทัล (International Society for Technology in Education [ISTE], 2016) เป็นองค์ประกอบสำคัญของการสร้างภูมิคุ้มกันภัยออนไลน์ เนื่องจากพฤติกรรมของผู้ใช้เทคโนโลยีมีผลโดยตรงต่อระดับความเสี่ยงด้านไซเบอร์ การส่งเสริมทักษะการรู้เท่าทันสื่อ การคิดเชิงวิพากษ์ การจัดการข้อมูลส่วนบุคคล และจริยธรรมดิจิทัล จึงเป็นแนวทางสำคัญในการลดความเสี่ยงและส่งเสริมการใช้เทคโนโลยีอย่างสร้างสรรค์ สถานศึกษาควรบูรณาการแนวคิดพลเมืองดิจิทัลในหลักสูตรการเรียนการสอน กิจกรรมพัฒนาผู้เรียน และวัฒนธรรมองค์กร โดยเน้นการเรียนรู้แบบมีส่วนร่วม การใช้กรณีศึกษา การจำลองสถานการณ์ และการเรียนรู้จากประสบการณ์จริง เพื่อให้ผู้เรียนสามารถนำความรู้ไปใช้ในชีวิตประจำวันได้อย่างเหมาะสมในระดับครูและบุคลากรทางการศึกษา การพัฒนาพลเมืองดิจิทัลควรมุ่งเน้นการเสริมสร้างสมรรถนะด้านการใช้เทคโนโลยี เพื่อการจัดการเรียนรู้ การคุ้มครองข้อมูลผู้เรียน การจัดการชั้นเรียนออนไลน์อย่างปลอดภัย และการเป็นแบบอย่างที่ดีในการใช้เทคโนโลยีอย่างมีจริยธรรม

มิติที่สาม มิติระบบความปลอดภัยไซเบอร์

การพัฒนาระบบความปลอดภัยไซเบอร์ (International Organization for Standardization [ISO], 2018) การพัฒนาระบบความปลอดภัยไซเบอร์ในสถานศึกษาเป็นองค์ประกอบเชิงโครงสร้างที่ช่วยสนับสนุน การสร้างภูมิคุ้มกันภัยออนไลน์อย่างยั่งยืน ระบบดังกล่าวครอบคลุมทั้งมาตรการทางเทคนิค มาตรการด้านการบริหารจัดการ และมาตรการด้านการสร้างความตระหนักรู้ มาตรการทางเทคนิค ได้แก่ การติดตั้งระบบป้องกันมัลแวร์ การเข้ารหัสข้อมูล การควบคุมสิทธิ์ การเข้าถึงข้อมูล การสำรองข้อมูล และการเฝ้าระวังภัยคุกคามทางไซเบอร์แบบเรียลไทม์ ขณะที่มาตรการด้านการบริหารจัดการเกี่ยวข้องกับการกำหนดนโยบายความปลอดภัยข้อมูล การจัดทำแผนรับมือเหตุการณ์ไซเบอร์ และการประเมินความเสี่ยงอย่างสม่ำเสมอ ในด้านการสร้างความตระหนักรู้ สถานศึกษาควรจัดกิจกรรมอบรม การประชาสัมพันธ์ และการสื่อสารภายในองค์กรอย่างต่อเนื่อง เพื่อให้ผู้เรียนและบุคลากร ตระหนักถึงความสำคัญของความปลอดภัยไซเบอร์ และสามารถปฏิบัติตนได้อย่างเหมาะสมเมื่อต้องเผชิญภัยออนไลน์

มิติที่สี่ มิตินโยบายและการบริหาร

มิตินโยบายและการบริหาร (Fullan, 2014) เป็นกลไกเชิงระบบที่ช่วยให้การดำเนินงานด้านความปลอดภัยดิจิทัล ในสถานศึกษามีความต่อเนื่องและยั่งยืน ผู้บริหารสถานศึกษามีบทบาทสำคัญในการกำหนดวิสัยทัศน์ นโยบาย และกลยุทธ์ด้านความปลอดภัยไซเบอร์ รวมทั้งการจัดสรรทรัพยากรเพื่อสนับสนุนการดำเนินงาน การกำหนดนโยบายควรครอบคลุมประเด็นสำคัญ เช่น การคุ้มครองข้อมูลส่วนบุคคล การใช้เทคโนโลยีอย่างเหมาะสม การจัดการเหตุการณ์ความปลอดภัยไซเบอร์ และการส่งเสริมวัฒนธรรมองค์กรที่ตระหนักถึงความปลอดภัยดิจิทัล นอกจากนี้ ควรมีการติดตามประเมินผลและปรับปรุงนโยบายอย่างต่อเนื่อง เพื่อให้สอดคล้องกับบริบทเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว ในระดับนโยบาย การศึกษาของประเทศ การสนับสนุนด้านงบประมาณ โครงสร้างพื้นฐานดิจิทัล การพัฒนาครู และการสร้างเครือข่ายความร่วมมือระหว่างหน่วยงาน เป็นปัจจัยสำคัญที่ช่วยเสริมสร้าง ระบบความปลอดภัยไซเบอร์ของสถานศึกษาอย่างเป็นรูปธรรม

โดยสรุป รูปแบบการบริหารเครือข่ายเพื่อเสริมสร้างภูมิคุ้มกันภัยออนไลน์ในสถานศึกษาประกอบด้วย การบูรณาการความร่วมมือเครือข่าย การพัฒนาพลเมืองดิจิทัล การเสริมสร้างระบบความปลอดภัยไซเบอร์

และการกำหนดนโยบายเชิงระบบ ซึ่งเมื่อดำเนินการอย่างสอดคล้องประสานกัน จะช่วยสร้างสภาพแวดล้อมการเรียนรู้ที่ปลอดภัย ส่งเสริมพฤติกรรมการใช้เทคโนโลยีอย่างรับผิดชอบ และสนับสนุนการพัฒนา คุณภาพการศึกษาในยุคดิจิทัลอย่างยั่งยืน

สรุปองค์ความรู้จากการศึกษา

การศึกษานี้สะท้อนให้เห็นว่า การบริหารเครือข่ายสถานศึกษาเพื่อเสริมสร้างภูมิคุ้มกันภัยออนไลน์เป็นกระบวนการเชิงระบบที่ต้องอาศัยการบูรณาการหลายมิติ ทั้งด้านการบริหารจัดการ เทคโนโลยีสารสนเทศ จริยธรรมดิจิทัล และความร่วมมือทางสังคม องค์ความรู้ที่ได้จากการสังเคราะห์ สามารถสรุปได้ว่า การบริหารเครือข่ายมีบทบาทสำคัญในการรับมือกับความท้าทายด้านความปลอดภัยไซเบอร์ในสถานศึกษา การพัฒนาความเป็นพลเมืองดิจิทัลของผู้เรียน ช่วยลดความเสี่ยงด้านพฤติกรรมออนไลน์ที่ไม่เหมาะสม ความจำเป็นของระบบความปลอดภัยไซเบอร์ต้องครอบคลุมทั้งมาตรการเชิงเทคนิคและมาตรการเชิงพฤติกรรม และนโยบายรวมถึงภาวะผู้นำเชิงกลยุทธ์เป็นกลไกสำคัญในการขับเคลื่อนการดำเนินงานให้เกิดความยั่งยืน นอกจากนี้ ยังพบว่าการสร้างวัฒนธรรมดิจิทัลเชิงบวกในสถานศึกษามีผลโดยตรง ต่อการพัฒนาทักษะการใช้เทคโนโลยีอย่างปลอดภัยและมีความรับผิดชอบต่อผู้เรียน การมีส่วนร่วมของผู้ปกครอง ชุมชน และหน่วยงานภายนอกช่วยเสริมสร้าง ระบบเฝ้าระวัง และป้องกันภัยออนไลน์ที่มีประสิทธิภาพมากขึ้น ซึ่งสะท้อนถึงแนวโน้มการบริหารการศึกษาในศตวรรษที่ 21 ที่เน้นการบริหารแบบเครือข่าย การมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย และการบูรณาการเทคโนโลยีดิจิทัล อย่างเป็นระบบเพื่อยกระดับคุณภาพการศึกษา

องค์ความรู้ที่ได้จากการศึกษานี้สามารถนำไปประยุกต์ใช้ได้หลายระดับ ได้แก่ ระดับนโยบาย ระดับสถานศึกษา และระดับชุมชนการเรียนรู้ทางวิชาชีพ โดยในระดับนโยบาย ผลการศึกษา สามารถใช้เป็นข้อมูลเชิงประจักษ์เพื่อสนับสนุนการกำหนดนโยบายด้านความปลอดภัยดิจิทัลในระบบ การศึกษา รวมถึงการพัฒนาแนวทางส่งเสริมพลเมืองดิจิทัลให้บูรณาการอยู่ในหลักสูตรการศึกษาทุกระดับ ซึ่งจะช่วยเสริมสร้างกรอบแนวคิดและมาตรการป้องกันภัยไซเบอร์อย่างเป็นระบบและมีทิศทางที่ชัดเจน ในระดับสถานศึกษา ผู้บริหารสถานศึกษาสามารถนำรูปแบบการบริหารเครือข่ายที่พัฒนาขึ้น ไปใช้เป็นกรอบแนวทางในการวางแผนกลยุทธ์ การสร้างความร่วมมือกับหน่วยงานภายนอก การพัฒนาโครงสร้างพื้นฐานด้านความปลอดภัยไซเบอร์ และการจัดกิจกรรมพัฒนาผู้เรียน ด้านการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัยและมีความรับผิดชอบต่อตนเอง ชุมชน และสังคม ครูผู้สอนสามารถนำองค์ความรู้ไปประยุกต์ใช้ในการออกแบบการจัดการเรียนรู้ที่ส่งเสริมการเรียนรู้เท่าทันสื่อ การคิดเชิงวิพากษ์ และการปลูกฝังจริยธรรมดิจิทัล เพื่อพัฒนาผู้เรียนให้มีทักษะการใช้เทคโนโลยีอย่างสร้างสรรค์ และปลอดภัย ในระดับชุมชนและสังคม การเผยแพร่องค์ความรู้ผ่านเครือข่ายวิชาชีพ การประชุมวิชาการ และการอบรมเชิงปฏิบัติการ จะช่วยสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์แก่ครู ผู้บริหาร ผู้ปกครอง และผู้มีส่วนเกี่ยวข้อง ตลอดจนส่งเสริมความร่วมมือระหว่างสถานศึกษา หน่วยงานภาครัฐ ภาคเอกชน และชุมชนอย่างต่อเนื่อง ซึ่งจะนำไปสู่การพัฒนากระบวนการนิเวศดิจิทัล (Castells, 2010) ทางการศึกษาที่มีความมั่นคง ปลอดภัย และยั่งยืนในระยะยาว

การอภิปรายเชิงทฤษฎีชี้ให้เห็นว่า แนวคิดการบริหารเครือข่ายสามารถอธิบายการจัดการความเสี่ยงดิจิทัลได้อย่างมีประสิทธิภาพ เนื่องจากเอื้อต่อการบูรณาการทรัพยากร ความรู้ ความเชี่ยวชาญจากหลายภาคส่วน ขณะเดียวกัน แนวคิดพลเมืองดิจิทัลช่วยอธิบายมิติด้านพฤติกรรม และจริยธรรมของผู้เรียน ซึ่งเป็นปัจจัยสำคัญต่อการป้องกันภัยออนไลน์ในระยะยาว ทั้งในมิติการใช้เทคโนโลยีอย่างรับผิดชอบ การเคารพสิทธิผู้อื่น การปฏิบัติตามกฎหมาย ในเชิงนโยบายผลการศึกษาชี้ให้เห็นว่า การพัฒนาความปลอดภัย

ดิจิทัลในสถานศึกษาควรดำเนินการ ควบคู่กันทั้งในระดับมหภาค และระดับจุลภาค โดยเน้นการกำหนดมาตรฐานความปลอดภัยไซเบอร์ การพัฒนาศักยภาพครูและบุคลากรทางการศึกษาด้านดิจิทัล การสนับสนุนโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ และการสร้างเครือข่ายความร่วมมือระหว่างภาคการศึกษา และภาคเทคโนโลยี เพื่อเสริมสร้างระบบการศึกษาที่ปลอดภัย และสอดคล้องกับการเปลี่ยนแปลงของสังคมดิจิทัล

ในเชิงทฤษฎี รูปแบบการบริหารเครือข่ายที่นำเสนอในบทความนี้สอดคล้องกับแนวคิดสังคมเครือข่ายของ Castells (2010) ซึ่งอธิบายว่าพลังอำนาจและการจัดการในยุคดิจิทัลไม่ได้ดำเนินผ่านโครงสร้างแบบลำดับชั้นเพียงอย่างเดียว หากแต่เกิดจากการเชื่อมโยงของหน่วยงานและเครือข่ายที่ทำงานร่วมกันอย่างยืดหยุ่น โมเดล 4 มิติที่เสนอจึงสะท้อนการปรับเปลี่ยนจากการบริหารแบบรวมศูนย์ไปสู่ การบริหารแบบเครือข่ายที่เน้นการมีส่วนร่วม การแลกเปลี่ยนทรัพยากร และการกำกับดูแลร่วมกัน (Provan & Kenis, 2008) โมเดลดังกล่าวแตกต่างจากแนวคิดเดิมที่มักเน้นเพียงมิติใดมิติหนึ่ง โดยบทความนี้มุ่งเสนอกรอบบูรณาการที่เชื่อมโยงมิติทางเทคโนโลยี สังคม และนโยบายเข้าไว้ด้วยกันในลักษณะของระบบนิเวศทางการศึกษาดิจิทัล (digital education ecosystem) อันประกอบด้วยผู้มีส่วนได้ส่วนเสียหลายระดับ

References

- Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes*, 50(2), 248–287.
[https://doi.org/10.1016/0749-5978\(91\)90022-L](https://doi.org/10.1016/0749-5978(91)90022-L)
- Bryman, A. (2012). *Social research methods* (4th ed.). Oxford University Press.
- Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.
- Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press.
- Fullan, M. (2014). *The principal: Three keys to maximizing impact*. Jossey-Bass.
- Hargreaves, A., & Fullan, M. (2012). *Professional capital: Transforming teaching in every school*. Teachers College Press.
- Hollandsworth, R., Dowdy, L., & Donovan, J. (2011). Digital citizenship in K–12: It takes a village. *TechTrends*, 55(4), 37–47. <https://doi.org/10.1007/s11528-011-0510-z>
- International Organization for Standardization. (2018). *ISO/IEC 27001:2018 information security management systems—Requirements*. <https://www.iso.org/standard/27001>
- International Society for Technology in Education. (2016). *ISTE standards for students*. <https://www.iste.org/standards>
- Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies. *Journal of Child Psychology and Psychiatry*, 55(6), 635–654. <https://doi.org/10.1111/jcpp.12197>
- Livingstone, S., Mascheroni, G., & Staksrud, E. (2017). *European research on children's internet use: Assessing the past and anticipating the future*. EU Kids Online, London School of Economics and Political Science.

- Muijs, D., West, M., & Ainscow, M. (2011). Why network? Theoretical perspectives on networking. *School Effectiveness and School Improvement*, 21(1), 5–26.
<https://doi.org/10.1080/09243450903569692>
- OECD. (2021). *21st-century readers: Developing literacy skills in a digital world*. OECD Publishing. <https://doi.org/10.1787/a83d84cb-en>
- Partnership for 21st Century Learning. (2015). *Framework for 21st century learning*.
<https://www.battelleforkids.org/networks/p21>
- Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, 18(2), 229–252.
<https://doi.org/10.1093/jopart/mum015>
- Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. Simon & Schuster.
- Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). International Society for Technology in Education.
- Selwyn, N. (2016). *Education and technology: Key issues and debates* (2nd ed.). Bloomsbury Academic.
- UNESCO. (2019). *Digital citizenship education in Asia-Pacific: Policy and practice*. UNESCO Bangkok. <https://bangkok.unesco.org/content/digital-citizenship-education-asia-pacific>