สรุปรายงานการพัฒนาข้าราชการการฝึกอบรม
หลักสูตร “ความเข้าใจและใช้เทคโนโลยีดิจิทัล ทักษะความฉลาดทางดิจิทัล
(Digital Literacy : Digital Intelligence)”
ผ่านระบบการเรียนออนไลน์ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA E-LEARNING)
โดย นางชริยา ใจคำ ตำแหน่ง เจ้าพนักงานธุรการชำนาญงาน
ฝ่ายบริหารทั่วไป ศูนย์ปฏิบัติการพัฒนาที่ดินโครงการหลวง สำนักงานพัฒนาที่ดินเขต ๖

หลักสูตร : ความเข้าใจและใช้เทคโนโลยีดิจิทัล ทักษะความฉลาดทางดิจิทัล
(Digital Literacy : Digital Intelligence)
ของหน่วยงาน : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA E-LEARNING)
วิทยากร : อาจารย์สุมนฒ์ จิรพัฒนพร
หัวหน้ากลุ่มงานวิชาการคอมพิวเตอร์
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏนครสวรรค์

คำอธิบายบทเรียน

“ความฉลาดทางดิจิทัล (DQ Digital Intelligence)” จาก DQ Institute ซึ่งเป็นสถาบันที่มีการพัฒนามาตรฐานระดับสากล เกี่ยวกับการให้ความรู้ด้านความฉลาดทางดิจิทัล มาวิเคราะห์ ปรับใช้ให้เหมาะสมกับบริบทของประเทศไทย โดยมีกรอบสมรรถนะ ๕ ด้าน คือ ๑) อัตลักษณ์ดิจิทัล (Digital Identity) ๒) การใช้เทคโนโลยีดิจิทัลอย่างเหมาะสม (Digital Use) ๓) การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security) ๔) การรู้เท่าทันดิจิทัล (Digital Literacy) และ ๕) การสื่อสารดิจิทัล (Digital Communication) โดยในแต่ละหัวข้อจะมีรายละเอียด สำหรับการพัฒนาความรู้ทักษะ และทัศนคติในการเป็นพลเมืองดิจิทัลที่มีคุณภาพ

วัตถุประสงค์

๑. เพื่อให้ผู้เรียนเข้าใจความหมายและเห็นความสำคัญ การสร้างความตระหนักรู้ในการใช้อินเทอร์เน็ต

๒. เพื่อให้ผู้เรียนมีความรู้การสร้างความตระหนักรู้ในการใช้อินเทอร์เน็ต รู้เท่าทันและมีความมั่นคงปลอดภัยเพื่อยกระดับวิถีชีวิตด้วยดิจิทัล

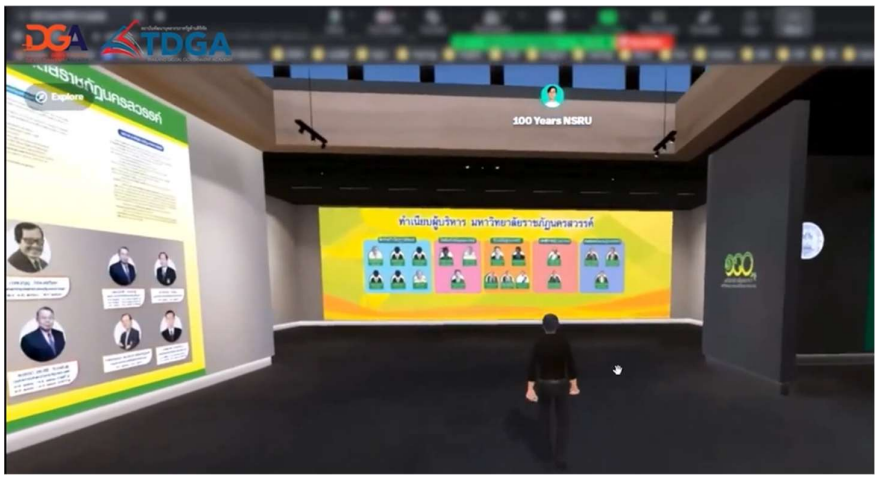
สรุปเนื้อหาการฝึกอบรม ประกอบด้วย ๖ หัวข้อ ดังนี้

หัวข้อที่ ๑ Digital Identity อัตลักษณ์ดิจิทัล

การเรียนรู้อัตลักษณ์ดิจิทัล (Digital Identity) ประกอบด้วย

๑.๑ โลกดิจิทัล คือ โลกเสมือนจริงซึ่งเพิ่มความสะดวก รวดเร็วในการหาข้อมูล การสื่อสาร การเผยแพร่เนื้อหารวมถึงการให้คำปรึกษาต่างๆ ซึ่งมีข้อด้อย เช่น ในเรื่องของการถ่ายทอดความรู้สึก การร่วมกิจกรรมที่ใช้การปฏิบัติและการทำธุรกรรมที่ต้องดำเนินการจริงอย่างธุรกรรมทางการเงิน

โลกดิจิทัลกับโลกความจริงจะต่างกันในเรื่องช่องทางการสื่อสาร เครื่องมืออิเล็กทรอนิกส์และเครือข่าย และมีความเสมือนที่ใกล้เคียงความจริงในเรื่องความเหมาะสมในการปฏิบัติ ได้แก่ การใช้งานอย่างมีมารยาท ยึดหลักจริยธรรมและต้องทำตามกฎหมาย



ตัวอย่าง : โปรแกรมที่สามารถสร้างโลกจำลองเสมือนจริง

๑.๒ อัตลักษณ์ดิจิทัล คือ ภาพลักษณ์และตัวตนในโลกดิจิทัลที่เกิดจากการเพยแพร่ข้อมูลบนโลกออนไลน์ที่ทำให้ผู้อื่นจดจำเราได้ในโลกของดิจิทัล ได้แก่

๑) ข้อมูลส่วนที่เป็นอันเดียวกับโลกความจริง ได้แก่ ชื่อ-นามสกุล รูปประจำตัว วันเกิด เลขบัตรประจำตัวประชาชน หรือเลขบัตรเครดิต

๒) กิจกรรม เช่น บัญชีอีเมล สถานที่เช็คอิน พฤติกรรม/ประวัติการใช้งาน

๓) ผลจากการสร้างอัตลักษณ์ดิจิทัล แบ่งได้ ๒ ทาง คือ

ทางบวก เช่น ผู้คนจดจำในทางที่ดี สร้างความสัมพันธ์ที่ดี เปิดโอกาสการสื่อสารต่างๆ

ทางลบ เช่น อาจถูกคนมุ่งร้าย เกิดภาพลักษณ์ในแง่ลบ ถูกโจรกรรมทางดิจิทัล ทำให้เสียโอกาสหรือมีผลต่อสภาพจิตใจ

ดังนั้น “การสร้างตัวตนดิจิทัลจะกลายเป็นตัวตนที่ไม่สามารถลบได้ จึงควรสร้างอัตลักษณ์ที่ดี”

๑.๓ ความเป็นส่วนตัว ในโลกดิจิทัล (Digital Privacy) ประกอบด้วย

๑) ข้อมูลส่วนตัว คือ ข้อมูลส่วนบุคคลที่เผยแพร่ได้โดยไม่เป็นอันตราย เช่น ชื่อ อายุ เพศ ความชอบต่างๆ สิ่งที่ไม่ควรเปิดเผย เช่น เลขบัญชีธนาคาร หมายเลขบัตรประจำตัวประชาชน เบอร์โทรศัพท์ ที่อยู่ และวันเกิด

๒) ข้อควรปฏิบัติเพื่อความปลอดภัย เช่น ไม่ตั้งค่าบัญชีเป็นสาธารณะ จัดการความปลอดภัยอุปกรณ์ ทำความเข้าใจเงื่อนไขของโปรแกรมที่ใช้งาน และตั้งรหัสผ่านรวมถึงการมีข้อมูลกู้คืนบัญชี

๓) กฎหมายที่เกี่ยวข้องกับสิทธิและความเป็นส่วนตัวในโลกดิจิทัล ได้แก่

- PDPA : กฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งระบุให้องค์กรหรือหน่วยงานที่เก็บข้อมูลของประชาชนต้องไม่นำข้อมูลส่วนตัวเหล่านั้นไปใช้โดยไม่ได้รับการยินยอม โดยจะคุ้มครองรวมถึงข้อมูลที่มีความอ่อนไหว (Sensitive Data) เช่น เชื้อชาติ เผ่าพันธุ์ ความเชื่อ ศาสนา ความเห็นทางการเมือง พฤติกรรมทางเพศและอื่นๆ

- บทลงโทษของผู้ที่ละเมิดสิทธิ์และความเป็นส่วนตัวของโลกดิจิทัลมี ดังนี้

๑) โทษทางอาญา : จำคุกไม่เกิน ๑ ปี และ/หรือปรับสูงสุด ๑ล้านบาท

๒) โทษทางแพ่ง : จ่ายสินไหมไม่เกิน ๒ เท่า ของสินไหมที่แท้จริง

๓) โทษทางปกครอง : ปรับไม่เกิน ๕ ล้านบาท

- พ.ร บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐ และ ๒๕๖๐

๑) ตามมาตรา ๙-๑๐ การแก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย มีโทษจำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑ แสนบาท หรือทั้งจำทั้งปรับ

๒) ตามมาตรา ๑๑ การส่งข้อมูลหรืออีเมลก่อกวนผู้อื่น หรือส่งอีเมลสแปม มีโทษจำคุกไม่เกิน ๒ ปี ปรับไม่เกิน ๔ หมื่นบาท หรือทั้งจำทั้งปรับ

๓) ตามมาตรา ๑๔ การนำข้อมูลที่ผิด พ.ร.บ. เข้าสู่ระบบคอมพิวเตอร์ มีโทษจำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๖ แสนบาท หรือทั้งจำทั้งปรับ

ดังนั้น แนวทางปฏิบัติเมื่อถูกคุกคามบนโลกดิจิทัล เช่น เมื่อถูกแฮกบัญชี จะสามารถทำการขอพิสูจน์ตัวตนดิจิทัล/ตั้งรหัสผ่านใหม่ หรือรายงานปัญหาไปยังเว็ปไซต์ และเมื่อกลับไปใช้งานให้ตั้งค่าการป้องกันระดับสูง

หัวข้อที่ ๒. Digital Use การใช้เทคโนโลยีอย่างเหมาะสม

การใช้เทคโนโลยีอย่างเหมาะสม (Digital Use) ประกอบด้วย

๒.๑ การใช้เทคโนโลยีอย่างสมดุล (Balanced Use of Technology) คือ การใช้งานหน้าจอนานเกินไปจะมีผลต่อสุขภาพ เช่น ทำให้สายตาเสีย ในกรณีที่อ่านตัวหนังสือที่เล็กเกินไปหรือหน้าจอมีแสงสว่างมากเกินไป หรือทำให้ปวดเมื่อยกล้ามเนื้อคอหรือแขนเมื่อใช้อุปกรณ์ในท่าทางที่ไม่เหมาะสม ซึ่งหลักการรักษาสมดุลเวลาใช้หน้าจอ มีหลักเกณฑ์ในการจัดสมดุลให้กับเวลาหน้าจอ มีดังนี้

๑) ในโลกความจริง : ให้คนเป็นเบอร์ ๑

๒) มีเป้าหมายทุกครั้ง : การใช้งานดิจิทัล

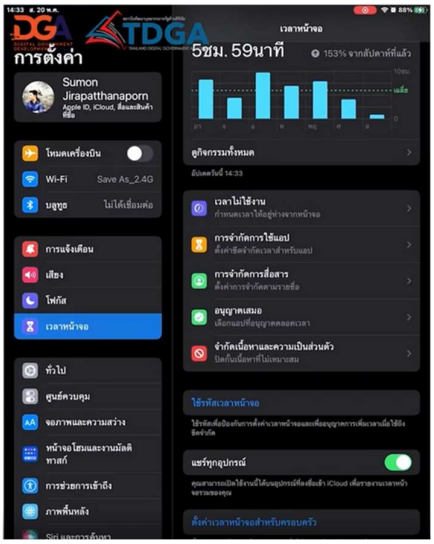
๓) ใช้ร่างกาย : ให้เป็นมาตรวัด

๔) เตรียมใจให้พร้อม : เมื่อเจอเวลาหน้าจอ

เครื่องมือแอพพลิเคชั่นที่สามารถเช็คระยะเวลาการใช้งานอุปกรณ์ได้ ในการบริหารจัดการหน้าจอ ได้แก่ การตั้งค่าระบบ Android : Digital Wellbeing และ ระบบ IOS

๑) วิธีการตั้งค่า ระบบ Android

๒) วิธีการตั้งค่า ระบบ IOS



วิธีการลดความเสี่ยงจากการใช้งานโทรศัพท์มือถือ ได้แก่ ยกให้มีระยะห่างจากสายตาประมาณ ๑๒-๑๘ นิ้ว , ยกตั้งศอกกับลำตัว, นั่งบนเก้าอี้มีพนักพิง, ไม่เล่นติดต่อกันเกิน ๑-๒ ชั่วโมง, พักสายตาและข้อมือทุก ๕-๑๐ นาที ,ปรับความสว่างหน้าจอให้เหมาะสม

ผลของการเสพติดเนื้อหา ประกอบด้วย

- อาการ : เข้าดูหลายๆ ครั้งใน ๑ วัน ถ้าไม่เข้าจะรู้สึกเหมือนขาดอะไรไป และคิดถึงเสมอเมื่อมีเวลาว่าง

- ผลต่อสุขภาพ : ภาวะซึมเศร้า เสี่ยงต่ออาการวิตกกังวล ขาดความยับยั้งชั่งใจ รู้สึกต่อต้านสังคม

๒.๒ การเอาใจใส่ทางดิจิทัล (Digital Empathy) มี ๒ สิ่งที่พึงกระทำ ดังนี้

สิ่งที่ควรทำ : การแสดงความคิดเห็นอย่างจริงใจ โดยตระหนักว่ามีคนอื่นที่สื่อสารนอกจากเราจึงควรใช้คำอย่างระมัดระวัง ใช้วิจารณญาณในการตีความและตอบโต้

สิ่งที่ไม่ควรทำ : ไม่ควรแสดงความเห็นหยอกล้อซึ่งอาจทำให้เกิดความเข้าใจผิดหรือการสื่อสารผิดพลาด ไม่ควรโพสต์ข้อความโวยวาย ต่อว่า ตำหนิหรือนินทาลับหลังผู้อื่น

เนื้อหาที่ควรระวัง - เนื้อหา/รูปภาพ ที่เป็นลิขสิทธิ์ของผู้อื่น

- เนื้อหา/รูปภาพ ที่อาจก่อให้เกิดความขัดแย้งด้านความเชื่อและศาสนา
- เนื้อหา/รูปภาพ ที่แสดงความรุนแรง ทารุณ
- เนื้อหา/รูปภาพ ที่แอบถ่ายหรือข้อมูลที่ไม่ได้รับอนุญาต

หัวข้อที่ ๓ Digital Security การจัดการความปลอดภัยในโลกดิจิทัล

การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security) ประกอบด้วย

๓.๑ การล่วงละเมิดทางไซเบอร์ (Cyber Abuse) คือ การแสดงพฤติกรรมที่เป็นอันตรายสร้างความรำคาญหรือสร้างความเสียหายให้กับผู้อื่นบนเครือข่ายออนไลน์ต่างๆ ทั้งด้านความรู้สึกและทรัพย์สิน ได้แก่

- การระรานทางไซเบอร์ (Cyber bullying) คือ การกลั่นแกล้ง ให้ร้าย ด่าว่า ข่มเหงหรือรังแกผู้อื่นในโลกดิจิทัล ผ่านช่องทางโซเชียลมีเดียต่างๆ

- การรังควานทางไซเบอร์ (Cyber Harassment) คือ การละเมิดที่รุนแรงมากขึ้นกว่าการระราน โดยการส่งข้อความหรือคอมเมนต์ทำร้ายจิตใจ

- การสะกดรอยตามทางไซเบอร์ (Cyber Stalking) คือ การติดต่อหรือการส่งข้อความซ้ำๆ อย่างต่อเนื่องจากบุคคลที่เราไม่ต้องการ เกิดจากแรงจูงใจต่างๆ

- การก่อกวน (Trolling) คือ การจงใจโพสต์หรือคอมเมนต์ที่ยั่วยุ ทำให้ตกใจ เสียอารมณ์ หรือทะเลาะกับบุคคลอื่น

สาเหตุของการถูกละเมิดทางไซเบอร์ คือ ความต้องการรังควานผู้ที่เป็นเป้าหมาย หรือผู้ขัดแย้งกันอยู่ หรือต้องการข่มขู่หรือสร้างความหวาดกลัว ให้กับผู้เป็นเป้าหมายหรือผู้ที่ขัดแย้งกันอย่างรุนแรง หรือติดตามไปประสงค์ร้ายในชีวิตจริง โดยมีสาเหตุภัยคุกคามทางไซเบอร์ ได้แก่

๑) การตั้งรหัสผ่านที่ง่ายเกินไป เช่น "password" มีผู้ใช้จำนวน ๔,๙๒๙,๑๑๓ บัญชี และ "๑๒๓๔๕๖" มีผู้ใช้จำนวน ๑,๕๒๓,๕๓๗ บัญชี

๒) โปรแกรมรักษาความปลอดภัยไม่ทำงานหรือทำงานไม่เต็มประสิทธิภาพ

๓) ความประมาท เช่น การกดลิงก์ที่ไม่รู้จัก

ผลกระทบของภัยคุกคามทางไซเบอร์ ประกอบด้วย ๒ ด้าน ดังนี้

๑) ด้านบุคคล : นำข้อมูลส่วนบุคคลไปใช้แอบอ้างเพื่อผลประโยชน์ต่างๆ

๒) ด้านอุปกรณ์ : สามารถโจมตีให้อุปกรณ์และระบบไม่สามารถใช้งานได้เพื่อเรียกเก็บเงินค่าไถ่

รูปแบบของการล่วงละเมิดทางไซเบอร์ ได้แก่

๑) การระรานทางไซเบอร์ : การกลั่นแกล้ง การให้ร้าย การด่าว่า การข่มเหง หรือ การรังแกผู้อื่นในโลดิจิทัล เช่น โซเชียลมีเดียต่างๆ

๒) การรังควานทางไซเบอร์ : การล่วงละเมิดทางไซเบอร์ที่ร้ายแรงกว่า พัฒนาการจากระบบทางไซเบอร์ โดยการส่งข้อความหรือคอมเมนต์ทำร้ายจิตใจ ถูกข่มขู่

๓) การสะกดรอยตามทางไซเบอร์ : การติดต่อหรือส่งข้อความมาซ้ำๆ อย่างต่อเนื่องจากบุคคลที่เราไม่ต้องการ เกิดจากแรงจูงใจต่างๆ มากมาย เช่น อารมณ์ ความรู้สึก

๔) การเกรียน : การจงใจโพสต์ หรือคอมเมนต์ข้อความที่ยั่วยุ ทำให้เสียอารมณ์ ตกใจ ทะเลาะกับคนอื่น การเกรียนมีหลายรูปแบบ แต่มักเป็นประเด็นขัดแย้ง

รูปแบบของภัยคุกคามทางไซเบอร์ ได้แก่ อีเมลอันตราย สแปม ฟิชชิ่ง มัลแวร์ ภัยจากการช้อปออนไลน์ และภัยจากการไม่สำรองข้อมูล ซึ่งมีเว็บไซต์ในการตรวจสอบภัยคุกคามทางดิจิทัล ดังนี้

๑) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)

๒) ศูนย์ปราบปรามอาชญากรรม

หัวข้อที่ ๔ Digital Literacy ด้านการรู้เท่าทันดิจิทัล

ด้านการรู้เท่าทันดิจิทัล Digital Literacy คือ ทักษะการเข้าใจ วิเคราะห์ ประเมิน และใช้สื่อดิจิทัลอย่างปลอดภัย มีวิจารณญาณ และสร้างสรรค์ โดยมุ่งเน้นการแยกแยะข้อมูลจริง-เท็จ ความเข้าใจบริบทสื่อ ลิขสิทธิ์ การป้องกันภัยคุกคามทางไซเบอร์ และการสื่อสารออนไลน์อย่างเหมาะสม เพื่อให้สามารถเอาตัวรอดและใช้งานเทคโนโลยีได้อย่างมีประสิทธิภาพในยุคปัจจุบัน ซึ่งประกอบด้วย

๔.๑ การใช้งานสื่อสารสนเทศ (Media and Information Use) เป็นแหล่งข้อมูลดิจิทัลสำหรับการค้นหา การนำเข้าข้อมูล เข้าถึง โดยผ่านระบบอินเตอร์เน็ต เช่น เว็บไซต์สุขภาพ ข่าวสาร บทความต่างๆ เพลง รายการบันเทิง และอื่นๆ

รูปแบบของแหล่งข้อมูลดิจิทัล แบ่งได้ดังนี้

๑) แหล่งที่เผยแพร่ข้อมูล : การสร้างหรือผลิตข้อมูลโดยเจ้าของแหล่งข้อมูล เช่น ข้อมูลจากเว็บไซต์โรงพยาบาล หน่วยงานรัฐ หรือเอกชนต่างๆ

๒) แบ่งตามสิทธิ์การเข้าถึงข้อมูล : - แหล่งข้อมูลที่เข้าถึงได้เสรี ไม่มีการจำกัดการเข้าถึงข้อมูล เช่น เว็บไซต์ที่เผยแพร่ข้อมูล

- แหล่งข้อมูลที่จำกัดการเข้าถึง ซึ่งสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตที่มีส่วนเกี่ยวข้อง เช่น ทะเบียนราษฎร์ ฐานข้อมูลภาครัฐ

๓) แบ่งตามประเภทของข้อมูล : - แหล่งข้อมูลเพื่อการศึกษาเรียนรู้

- แหล่งข้อมูลเพื่อความบันเทิง
- แหล่งข้อมูลด้านสุขภาพ
- แหล่งข้อมูลด้านธุรกรรมและการเงิน
- แหล่งข้อมูลด้านเศรษฐศาสตร์และเศรษฐกิจ

๔.๒ ผู้จัดทำสื่อและสารสนเทศ (Media and Information Create) เกี่ยวกับเนื้อหาทางด้านสื่อดิจิทัล โดยมีทั้งหมด ๖ ประเภท ดังนี้

๑) เนื้อหาดิจิทัลเกี่ยวกับสุขภาพอนามัย : เกี่ยวกับการดูแลสุขภาพ สาเหตุการเกิดโรคต่างๆ วิธีการป้องกันการเกิดโรคภัย จัดทำขึ้นโดยหน่วยงานสุขภาพ

๒) เนื้อหาดิจิทัลเกี่ยวกับข้อมูลภาครัฐ : การให้บริการข้อมูลต่างๆ ของภาครัฐ สิทธิและหน้าที่ของประชาชนในเรื่องต่างๆ กฎหมาย ระเบียบ เป็นต้น

๓) เนื้อหาดิจิทัลเพื่อความบันเทิง : ตอบสนองความต้องการด้านความบันเทิง เช่น ภาพยนตร์ นิยาย จัดทำขึ้นโดยบริษัทหรือผู้ประกอบการด้านบันเทิง

๔) เนื้อหาดิจิทัลด้านการตลาด : เพื่อซื้อขายหรือสร้างแรงจูงใจ ให้เกิดการซื้อสินค้าหรือบริการ ผลิตโดยบริษัทหรือร้านที่ทำธุรกิจ

๕) เนื้อหาดิจิทัลด้านการศึกษาและการเรียนรู้ : การศึกษาในระบบและการศึกษาเรียนรู้ตามอัธยาศัย จัดทำขึ้นโดยสถาบันการศึกษา หรือผู้เชี่ยวชาญ

๖) เนื้อหาดิจิทัลด้านข่าวสาร : รายงานความเคลื่อนไหวที่เกิดขึ้นในสังคม อาจจะเป็นด้านธุรกิจ ด้านการศึกษา หรือเหตุการณ์ทั่วไป

หัวข้อที่ ๕ Digital Communication ด้านการสื่อสารดิจิทัล

ด้านการสื่อสารดิจิทัล Digital Communication คือ การแลกเปลี่ยนข้อมูลผ่านเทคโนโลยีและอุปกรณ์อิเล็กทรอนิกส์ เช่น อีเมล โซเชียลมีเดีย และแอปแชท แบบเรียลไทม์ จุดเด่นคือความรวดเร็ว โต้ตอบได้สูง มีส่วนร่วมมากขึ้น และลดลำดับชั้นการสื่อสาร ทักษะสำคัญประกอบด้วยการเลือกใช้เครื่องมือให้เหมาะสม, การเข้าใจ, Digital Footprint การวิเคราะห์ข้อมูลอย่างมีวิจารณญาณ และการรักษาความปลอดภัยออนไลน์

หัวใจสำคัญของการสื่อสารดิจิทัล ประกอบด้วย

๑. ร่องรอยดิจิทัล Digital Footprint คือ ข้อมูลพฤติกรรมที่เราทิ้งไว้จากการใช้งานอินเทอร์เน็ต ทั้งที่ตั้งใจ (Active) เช่น การโพสต์, ไลค์, แชร์, สมัครบริการ และที่ไม่ตั้งใจ (Passive) เช่น ประวัติการเข้าชมเว็บไซต์, IP Address, คุกกี้ ซึ่งบันทึกและติดตามย้อนกลับได้ ร่องรอยเหล่านี้มีผลต่อชื่อเสียง, การสมัครงาน และเสี่ยงต่อการถูกมิจฉาชีพนำไปใช้หากจัดการไม่ดี

วิธีการดูแลร่องรอยทางดิจิทัล มี ๕ วิธี ดังนี้

๑) คิดก่อนคลิก: ตระหนักถึงผลที่จะตามมาเสมอ ก่อนจะโพสต์หรือแชร์สิ่งใด

๒) ตั้งค่าความเป็นส่วนตัว: จำกัดการเข้าถึงข้อมูลส่วนตัวในโซเชียลมีเดีย

๓) ลบ/ล้างข้อมูล: ทำความสะอาดประวัติการค้นหาและคุกกี้เป็นประจำ

๔) ค้นหาตัวเอง: ค้นหาชื่อตัวเองบน Google เพื่อดูว่ามีข้อมูลใดเปิดเผยอยู่บ้าง

๕) ตรวจสอบสิทธิ์: เข้าใจสิทธิ์ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๒. การมีปฏิสัมพันธ์และการส้รางความร่วมมือ คือ ทักษะการสื่อสารบนโลกดิจิทัล ช่วยให้การสื่อสารอย่างมีประสิทธิภาพ การสร้างความไว้วางใจ และการเข้าถึงข้อมูลอย่างถูกต้องและปลอดภัย การสื่อสารผ่านช่องทางดิจิทัล เช่น อีเมล โซเชียลมีเดีย เว็บไซต์ แชท ฯลฯ ทักษะการสื่อสารบนโลกดิจิทัลมีความสำคัญต่อการใช้ชีวิตในยุคปัจจุบัน การสื่อสารบนโลกดิจิทัลมีประโยชน์มากมาย เช่น การเชื่อมต่อกับผู้คนจากทุกมุมโลก การแบ่งปันข้อมูลและความรู้ การสร้างความเข้าใจและความร่วมมือ และการสร้างความสัมพันธ์ทางธุรกิจ เพื่อเติมเต็มประสบการณ์ในการสื่อสารของเราและผู้อื่น

การสื่อสารบนโลกดิจิทัลต้องใช้ทักษะที่แตกต่างจากการสื่อสารแบบดั้งเดิม เนื่องจากการสื่อสารบนโลกดิจิทัลเกี่ยวข้องกับการใช้เทคโนโลยีและสื่อโซเชียล ทักษะที่สำคัญประกอบไปด้วยการเข้าใจและใช้ประโยชน์จากเทคโนโลยี การสื่อสารอย่างมีประสิทธิภาพ การสร้างความไว้วางใจ และการเข้าถึงข้อมูลอย่างถูกต้องและปลอดภัย

องค์ประกอบสำคัญของ Digital Communication มีดังนี้

๑. การรู้จักเครื่องมือดิจิทัล : เข้าใจวิธีใช้เครื่องมือดิจิทัลต่างๆ เช่น อีเมล โซเชียลมีเดีย เว็บไซต์ แชท ฯลฯ โดยเฉพาะคุณลักษณะสำคัญของแต่ละเครื่องมือว่ามีข้อดี และข้อจำกัดอย่างไร และเลือกใช้ได้อย่างเหมาะสมต่อการสื่อสาร

๒. เข้าใจเรื่องรอยเท้าดิจิทัล Digital Footprint : ร่องรอยการใช้งานบนโลกออนไลน์ เปรียบเสมือนรอยเท้าที่เราทิ้งไว้ทุกครั้งที่ใช้อินเทอร์เน็ต เช่นข้อมูลส่วนตัว ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล รูปภาพ ฯลฯ กิจกรรมออนไลน์อย่างการ โพสต์ แชร์ คอมเมนต์ กดไลค์ ประวัติการค้นหา การโต้ตอบออนไลน์ผ่านข้อความส่วนตัว การสนทนาในกลุ่ม รวมถึงการใช้งานเว็บไซต์ ซึ่งจะถูกบันทึกประวัติการเข้าชมเว็บไซต์ คุกกี้

๓. การสื่อสารอย่างมีวิจารณญาณ : วิเคราะห์ข้อมูล ตรวจสอบความถูกต้อง และประเมินความน่าเชื่อถือของข้อมูล ก่อนเลือกที่จะตอบโต้หรือสื่อสารอย่างเหมาะสมตามบริบทของการสื่อสาร

๔. การรักษาความปลอดภัยบนโลกออนไลน์ : เข้าใจและปฏิบัติตามแนวทางการรักษาความปลอดภัยข้อมูลส่วนตัว โดยเลือกที่จะไม่ทิ้งร่องรอยในพื้นที่เสี่ยงเช่น เว็บไซต์ที่ไม่น่าไว้วางใจ หรือเกี่ยวข้องกับพื้นที่ออนไลน์ที่เสี่ยงต่อการกระทำที่ผิดกฎหมาย

ดังนั้น การสื่อสารบนโลกดิจิทัลเป็นสิ่งสำคัญที่ต้องพัฒนา เพื่อให้สามารถเชื่อมต่อกับผู้คนและองค์กรในโลกดิจิทัลได้อย่างมีประสิทธิภาพ ทักษะการสื่อสารบนโลกดิจิทัลมีความหลากหลาย เช่น การใช้เทคโนโลยีและสื่อโซเชียลให้เกิดประโยชน์ การใช้เทคนิคการสื่อสารที่เหมาะสม และการใช้ประโยชน์จากการสื่อสารบนโลกดิจิทัลให้เกิดประโยชน์ต่อการสื่อสารของเราและผู้อื่น

หัวข้อที่ ๖ Digital Disruption การปรับตัวในยุคดิจิทัล

การปรับตัวในยุคดิจิทัล Digital Disruption คือ การเปลี่ยนแปลงฉับพลันที่เทคโนโลยีใหม่ (เช่น AI แพลตฟอร์มออนไลน์) เข้ามาแทนที่รูปแบบธุรกิจเดิม ทำให้ธุรกิจต้องปรับตัวโดยการทำ Digital Transformationใช้ข้อมูลวิเคราะห์พฤติกรรมลูกค้าและสร้างประสบการณ์แบบไร้รอยต่อ (Seamless Experience) การปรับตัวเน้นความคล่องตัว การสร้างมูลค่าเพิ่มและการทำ Online-Offline Integration

สรุป Technology Literacy ไม่ใช่เพียงการใช้อุปกรณ์ดิจิทัลอย่างชำนาญเท่านั้น แต่หมายรวมถึง ความสามารถในการวิเคราะห์ประเมินข้อมูล ใช้งานเทคโนโลยีอย่างมีจริยธรรม ปลอดภัย และสามารถปรับตัวในโลกที่เปลี่ยนแปลงอย่างรวดเร็ว การส่งเสริมทักษะนี้ในทุกช่วงวัย ถือเป็นหัวใจสำคัญที่จะช่วยให้บุคคลและสังคมพร้อมรับมือกับความท้าทายในศตวรรษนี้ได้อย่างมั่นคง และสามารถปรับใช้ให้เหมาะสมกับบริบทของประเทศไทย โดยมีกรอบสมรรถนะ ๕ ด้าน รวมทั้งทัศนคติในการเป็นพลเมืองดิจิทัลที่มีคุณภาพ

ประโยชน์ที่ได้รับจากการฝึกอบรม

ในยุคดิจิทัลที่เทคโนโลยีมีบทบาทสำคัญในชีวิตประจำวันและทุกภาคส่วนของสังคม ความสามารถในการใช้เทคโนโลยีดิจิทัลอย่างถูกต้อง ปลอดภัย และมีประสิทธิภาพ หรือที่เรียกว่า Technology Literacy เป็นทักษะจำเป็นสำหรับการดำรงชีวิต ความรู้และทักษะนี้ช่วยให้บุคคลสามารถเข้าถึงข้อมูล วิเคราะห์ ใช้สื่อเทคโนโลยีอย่างรับผิดชอบ รวมถึงสื่อสารและแก้ปัญหาในบริบทดิจิทัลได้อย่างเหมาะสม ทำให้การมีทักษะช่วยเพิ่มโอกาสในการเข้าถึงข้อมูลและบริการที่สำคัญให้กับตนเองและหน่วยงาน เช่น การทำงานออนไลน์ การทำงานจากระยะไกล การให้บริการประชาชนด้านสาธารณะดิจิทัล หรือการสื่อสารและการทำงานร่วมกัน (Digital Communication and Collaboration) โดยใช้เครื่องมือดิจิทัลในการติดต่อสื่อสารและทำงานร่วมกับผู้อื่นได้อย่างมีประสิทธิภาพอีกทั้งยังช่วยลดช่องว่างทางดิจิทัล (Digital Divide) ที่เกิดจากความไม่เท่าเทียมในการเข้าถึงและใช้เทคโนโลยี ส่งผลให้สังคมมีความเป็นธรรมและครอบคลุมมากขึ้น ประกอบกับ โลกที่เปลี่ยนแปลงอย่างรวดเร็วและพึ่งพาเทคโนโลยีมากขึ้น ทำให้ทุกคนต้องมีความสามารถในการใช้อุปกรณ์ดิจิทัลทั้งสมาร์ทโฟน แท็บเล็ต คอมพิวเตอร์ รวมถึงเครื่องมือสื่อสารออนไลน์อย่างเหมาะสม เพราะเทคโนโลยีไม่เพียงอำนวยความสะดวก แต่ยังเปิดโอกาสในการเรียนรู้ การทำงาน และการเชื่อมต่อกับผู้คนทั่วโลก นอกจากนี้ การมีความเข้าใจด้านความปลอดภัยไซเบอร์ (Cybersecurity) ช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ การรั่วไหลของข้อมูลส่วนตัว หรือการถูกหลอกลวงในโลกออนไลน์

(นางชริยา ใจคำ)
เจ้าพนักงานธุรการชำนาญงาน
ผู้เข้ารับการฝึกอบรม
วันที่ ๑๓ มีนาคม ๒๕๖๙