พลเมืองดิจิทัล

ความหมายและคุณลักษณะเบื้องต้นของพลเมืองดิจิทัล

การใช้เทคโนโลยีสารสนเทศอย่างสม่ำเสมอและมีประสิทธิภาพเป็นคุณลักษณะเบื้องต้นของการเป็นพลเมืองในยุคดิจิทัลนอกจากนี้บุคคลผู้นั้นจะต้องมีทักษะและความรู้ที่หลากหลายในการใช้อินเทอร์เน็ตผ่านอุปกรณ์และช่องทางการสื่อสารประเภทต่างๆ เช่น โซเชียลเนตเวิร์ก (Facebook, Twitter, Instagram, Line) และอุปกรณ์อิเล็กทรอนิกส์รูปแบบใหม่ (แท็บเล็ต และมือถือสมาร์ทโฟน) เป็นต้น อย่างไรก็ตามมีผู้ตั้งข้อสังเกตว่าทักษะการใช้อินเทอร์เนตและเทคโนโลยีสารสนเทศเพื่อประโยชน์ในการดำรงชีวิตประจำวันไม่เพียงพอต่อคุณลักษณะของการเป็นพลเมืองดิจิตอลที่สมบูรณ์ หากแต่บุคคลผู้นั้นจะต้องใช้เทคโนโลยีดังกล่าว ในทางที่จะก่อให้เกิดประโยชน์ต่อบุคคลอื่นและสังคม เช่น การเคารพสิทธิและหน้าที่ของผู้อื่นตลอดจนการใช้เทคโนโลยีเพื่อสื่อสารกับภาครัฐและภาคเอกชนเพื่อก่อให้เกิดการเปลี่ยนแปลงในทางที่ดีและถูกต้อง (https://www.stou.ac.th/study/sumrit/1-59(500)/page2-1-59(500).html)

ความเป็นพลเมืองดิจิทัล (Digital Citizenship) เป็นพลเมืองที่มีความสามารถในการใช้อินเทอร์เน็ตในการบริหารจัดการ ควบคุม กำกับตน รู้ผิดรู้ถูก และรู้เท่าทัน เป็นบรรทัดฐานในการใช้เทคโนโลยีดิจิทัลอย่างเหมาะสม มีความรับผิดชอบ เรียนรู้ที่จะใช้เทคโนโลยีอย่างชาญฉลาด และปลอดภัย พลเมืองดิจิทัลจึงต้องตระหนักถึงโอกาสและความเสี่ยงในโลกดิจิทัล เข้าใจถึงสิทธิและความรับผิดชอบในโลกออนไลน์ ความเป็นพลเมืองดิจิทัล (https://www.scimath.org/article-technology/item/8659-2018-09-11-07-58-08)

ความเป็นพลเมืองดิจิทัลสามารถแยกองค์ประกอบได้เป็น 4 มิติ ดังนี้

1. มิติการรักษาอัตลักษณ์และข้อมูลส่วนบุคคล

การสร้างอัตลักษณ์ออนไลน์ถือเป็นปรากฏการณ์ใหม่ ที่ทำให้บุคคลสามารถแสดงออกถึงความเป็นตัวตนของตนเองต่อสังคมภายนอก ด้วยการอาศัยช่องทางการสื่อสารผ่านเว็บไซต์เครือข่ายสังคมเพื่ออธิบายรูปแบบใหม่ของการสื่อสารแบบมีปฏิสัมพันธ์ทางอินเทอร์เน็ตที่ทำให้เกิดการแสดงออกเกี่ยวกับตัวตนผ่านเว็บไซต์เครือข่ายสังคมต่าง ๆ เพื่อการสื่อสารและเชื่อมต่อความสัมพันธ์กับบุคคลอื่น การที่ผู้ใช้ปรับตัวให้เข้ากับเทคโนโลยีสื่อใหม่และการใช้กลยุทธ์ต่าง ๆ เพื่อนำเสนอตัวตนบนโลกออนไลน์ พลเมืองดิจิทัลจะต้องมีความตระหนักในความเท่าเทียมกันทางดิจิทัล การรักษาความปลอดภัยของข้อมูลตนเองในสังคมดิจิทัล ที่มีความจำเป็นจะต้องบริหารจัดการข้อมูลของตนเอง รู้ว่าข้อมูลใดควรเผยแพร่และข้อมูลใดไม่ควรเผยแพร่ การปกป้องข้อมูลส่วนบุคคล การจัดการกับความเสี่ยงของข้อมูลของตนในสื่อสังคมดิจิทัล

2. มิติของกิจกรรมบนสื่อสังคมดิจิทัล

พลเมืองดิจิทัลทีความจำเป็นต้องมีความสามารถในการจัดการธุรกรรมการเงินทางอินเทอร์เน็ต เช่น การซื้อขายสินค้าในอินเทอร์เน็ต บัตรเครดิตอิเล็กทรอนิกส์ การค้าแบบดิจิทัล การเมือง เศรษฐกิจ การมีส่วนร่วมวัฒนธรรมพลเมืองดิจิทัลต้องรู้จักใช้ศักยภาพของอินเทอร์เน็ตในการมีส่วนร่วมทางการเมือง เศรษฐกิจและสังคม อินเทอร์เน็ตเป็นได้ทั้งเครื่องมือเพิ่มการมีส่วนร่วมทางการเมืองในระบบ เช่น รัฐบาลใช้อินเทอร์เน็ตในการรับฟังความเห็นของประชาชนก่อนออกกฎหมาย การลงคะแนนเสียงอิเล็กทรอนิกส์ หรือการยื่นคำร้องออนไลน์ อีกทั้งพลเมืองดิจิทัลจะต้องการรักษาความสัมพันธ์ที่ดีกับคนในสังคมดิจิทัล มีน้ำใจการแสดงความเห็นอกเห็นใจ เสียใจ เห็นด้วย ไม่เห็นด้วย ยินดี สนุกสนาน เพื่อสานสัมพันธ์กับผู้คนในโลกออนไลน์ การสร้างความสัมพันธ์ระหว่างตนเองกับสังคมและสิ่งแวดล้อมเพื่อให้สามารถอยู่ในสังคมได้อย่างมีความสุข

3. มิติทักษะและความสามารถในสภาพแวดล้อมดิจิทัล

พลเมืองดิจิทัลต้องมีความรู้ความสามารถในการเข้าถึง ใช้ สร้างสรรค์ ประเมิน สังเคราะห์ และสื่อสารข้อมูลข่าวสารผ่านเครื่องมือดิจิทัล ดังนั้นพลเมืองยุคใหม่จึงต้องมีความรู้ด้านเทคนิคในการเข้าถึงและใช้

เครื่องมือดิจิทัล เช่น คอมพิวเตอร์ สมาร์ตโฟน แท็บเล็ต ได้อย่างเชี่ยวชาญ รวมถึงทักษะในการรู้คิดขั้นสูง เช่น ทักษะการคิดอย่างมีวิจารณญาณ ซึ่งจำเป็นต่อการเลือก จัดประเภท วิเคราะห์ ตีความ และเข้าใจข้อมูลข่าวสาร มีความรู้และทักษะในสภาพแวดล้อมดิจิทัล การรู้ดิจิทัลโดยมุ่งให้เป็นผู้ใช้ที่ดี เป็นผู้เข้าใจบริบทที่ดี และเป็นผู้สร้างเนื้อหาทางดิจิทัลที่ดี ในสภาพแวดล้อมสังคมดิจิทัล

4. มิติจริยธรรมทางดิจิทัล

พลเมืองดิจิทัล จะต้องเป็นผู้รู้กฎหมายที่เกี่ยวกับคอมพิวเตอร์ การกระทำความผิดทางคอมพิวเตอร์ การใช้เทคโนโลยีอย่างรู้จริยธรรม รู้จักคุณค่าและจริยธรรมจากการใช้เทคโนโลยี มีความรู้ในงานลิขสิทธิ์และเคารพทรัพย์สินทางปัญญาของผู้อื่น และการปกป้องตนเองและชุมชน มีความรับผิดชอบทางดิจิทัล รู้จักสิทธิเสรีภาพให้เกียรติในการพูดการกระทำในสังคมดิจิทัล มารยาททางดิจิทัล เข้าใจถึงการรับความในการบริหารจัดการความเสี่ยงในโลกออนไลน์ เช่น การไม่ไปรังแกและสามารถจัดการกับการถูกรังแกบนโลกไซเบอร์ (Cyberbullying) รวมไปถึงการเกี้ยวพาราสี การเหยียดผิว-เหยียดชนชั้น รวมไปถึงเนื้อหาต่าง ๆ ที่สุ่มเสี่ยงเช่น เนื้อหาที่มีความรุนแรง โป๊เปลือย ลามกหยาบคายด้วย

กล่าวโดยสรุป พลเมืองดิจิทัลที่ดีจะต้องมีทักษะทางดิจิทัลมีชุดทักษะและความรู้ทั้งในเชิงเทคโนโลยีและการคิดขั้นสูง ในการรักษาอัตลักษณ์และข้อมูลส่วนบุคคลของตนเอง เคารพสิทธิเสรีภาพการใช้ข้อมูลทั้งของตนเองและผู้อื่น สามารถบริหารจัดการกิจกรรมบนสื่อสังคมดิจิทัล รวมถึงการสร้างความสัมพันธ์ระหว่างตนเองกับสังคมและสิ่งแวดล้อม มีความรู้ด้านเทคนิคในการเข้าถึงและใช้เครื่องมือดิจิทัล มีทักษะการคิดอย่างมีวิจารณญาณ รู้จักคุณค่าและจริยธรรมจากการใช้เทคโนโลยี มีความรู้ในงานลิขสิทธิ์และเคารพทรัพย์สินทางปัญญาของผู้อื่น การปกป้องตนเองและชุมชน และเกิดความรับผิดชอบทางดิจิทัล (https://www.scimath.org/article-technology/item/8659-2018-09-11-07-58-08)

1. สิทธิและความรับผิดชอบยุคดิจิทัล

คำจำกัดความสิทธิและเสรีภาพ

พจนานุกรมฉบับราชบัณฑิตยสถาน ได้ให้ความหมายคำว่า **"สิทธิ"** หมายถึงความสำเร็จหรืออำนาจที่จะกระทำการใดๆได้อย่างอิสระ โดยได้รับการรับรองจาก"เสรีภาพ"หมายถึง อำนาจตัดสินใจด้วยตนเองของมนุษย์ที่จะเลือกทำเป็น พฤติกรรมของตนเองโดยไม่มีบุคคลอื่นใด อ้างหรือใช้อำนาจแทรกแซงเกี่ยวข้องกับการตัดสินใจนั้น

รัฐธรรมนูญแห่งราชอาณาจักรสยามพ.ศ. 2475 บัญญัติไว้เป็นครั้งแรกว่า "บุคคลย่อมมีเสรีภาพบริบูรณ์ในการนับถือศาสนาหรือลัทธิใดๆ และมีเสรีภาพในการปฏิบัติพิธีกรรมตามความเชื่อของตนเมื่อไม่เป็นปฏิปักษ์ต่อหน้าที่ของพลเมืองและไม่เป็นการขัดต่อความสงบเรียบร้อยหรือศีลธรรมของประชาชน"และ" ภายในบังคับแห่งกฎหมายบุคคลย่อมมีเสรีภาพบริบูรณ์ในร่างกาย เคหสถาน ทรัพย์สินการพูด การเขียน การโฆษณาการศึกษา อบรม การประชุมโดยเปิดเผย การตั้งสมาคม การอาชีพ "

2. การเข้าถึงดิจิทัล (Digital Access)

การรู้ดิจิทัล (Digital literacy) คืออะไร

Digital literacy หรือทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล เป็นทักษะด้านดิจิทัลพื้นฐานที่จะเป็นตัวช่วยสำคัญในการปฏิบัติงาน การสื่อสาร และการทำงานร่วมกันกับผู้อื่นในลักษณะ “ทำน้อย ได้มาก” หรือ “Work less but get more impact” และช่วยสร้างคุณค่า (Value Co-creation) และความคุ้มค่าในการดำเนินงาน (Economy of Scale) เพื่อการก้าวไปสู่การเป็นประเทศไทย 4.0 อีกทั้งยังเป็นเครื่องมือช่วยให้

บุคลากร สามารถเรียนรู้และพัฒนาตนเองเพื่อให้ได้รับโอกาสการทำงานที่ดีและเติบโตก้าวหน้าในอาชีพ (Learn and Growth)

เข้าถึง (Access) คือ การเข้าถึงและใช้ประโยชน์จากเทคโนโลยีดิจิทัล และข้อมูลข่าวสาร เป็นฐานรากในการพัฒนา การสร้างความเจริญเติบโตทางเศรษฐกิจ ผู้เรียนจำเป็นต้องเข้าใจอินเทอร์เน็ตและการเข้าถึงอินเทอร์เน็ตด้วยช่องทางต่าง ๆ รวมถึง ข้อดีข้อเสียของแต่ละช่องทางได้ เพื่อให้สามารถใช้ Search Engine ค้นหาข้อมูลที่ต้องการจาก อินเทอร์เน็ตได้อย่างมีประสิทธิภาพ นอกจากนี้ยังจำเป็นต้องเข้าใจสื่อทางดิจิทัลชนิดต่าง ๆ รวมถึง การนำไปประยุกต์ใช้

3. การสื่อสารยุคดิจิทัล (Digital Communication)

การสื่อสารยุคดิจิทัล หมายถึง การสื่อสารระหว่างบุคคลและสังคมผ่านเครือข่ายอินเทอร์เน็ตโดยการใช้อุปกรณ์ดิจิทัลต่าง ๆ เช่น คอมพิวเตอร์ โทรศัพท์ สมาร์ตโฟนโทรศัพท์ดิจิทัล เป็นต้น และผ่านช่องทางการสื่อสารดิจิทัล หรือดิจิทัลแพลตฟอร์ม (Digital Platform) (https://skrudl.skru.ac.th/file/1.3.pdf)

- การสื่อสารแบบด้วยตัวอักษร (Text)
- การสื่อสารแบบด้วยภาพนิ่ง (Image)
- การสื่อสารด้วยภาพเชิงสัญลักษณ์ (Emoticon และ Sticker)
- การสื่อสารแบบด้วยภาพเคลื่อนไหวจริง (Video)
- การสื่อสารแบบด้วยภาพเคลื่อนไหวจริงแบบทันที่ทันใด (Real Time Video/Live Video)

แนวทางการสื่อสารยุคดิจิทัลเพื่อสื่อสารให้ได้ความหมายและสร้างคุณค่าการสื่อสารด้วยรูปแบบใดก็ตามผู้ส่งสารหรือผู้สื่อสารต้องคำนึงหลักการสำคัญ 3 ข้อ ได้แก่แก่

- มีความรับผิดชอบ

คำนึงถึงผลกระทบที่จะตามมาหลังจากสื่อสารนั้นเกิดขึ้นไปแล้วหรือสารถูกเผยแพร่ซึ่งอาจจะก่อให้เกิดผลด้านบวกและด้านลบต่อบุคคลและสังคม

- มีความประณีต

การเลือกระดับของภาษาการเลือกสรรถ้อยคำการใช้สำนวนทางภาษา การจัดองค์ประกอบการจัดรูปแบบ ลำดับเนื้อหา และแสดงเนื้อหาสาระ ความหมายโดยสารที่ถูกส่งออกไปต้องมีความกระชับ ความไพเราะ สุภาพเพื่อให้บรรลุตามจุดประสงค์ของการสื่อสาร รวมถึงเลือกใช้ช่องทางและอุปกรณ์ ที่เหมาะสม

- ถูกกาลเทศะ

การคำนึงถึงผู้รับสารจุดประสงค์การสื่อสาร กฎระเบียบข้อบังคับ ระยะเวลา เครื่องมือเทคโนโลยีและสถานการณ์แวดล้อม ตัวแปรเหล่านี้จะเป็นตัวกำหนดความเหมาะสมของสารและองค์ประกอบการสื่อสาร

4. ความปลอดภัยยุคดิจิทัล (Digital Safety)

คือการเข้าใจความรู้พื้นฐานทั่วไปของ ความ ปลอดภัยบนโลกอินเทอร์เน็ต โดย จะมีอันตรายที่มาจากผู้ไม่ประสงค์ดีใน โลก อินเทอร์เน็ต เครือข่ายสังคม ออนไลน์ ได้อย่างถูกต้องและปลอดภัย เพื่อการ หลีกเลี่ยงภัยคุกคาม และรับมือ กับภัยอันตรายในโลกดิจิทัล (https://skrudl.skru.ac.th/file/1.4.pdf)

- รอยเท้าดิจิทัล (Digital Footprint)

คือ ร่องรอยที่ผู้ใช้อินเทอร์เน็ตและโลกไซเบอร์กระทำการต่าง ๆ ในโลกดิจิทัล เช่น การใช้งานอัปโหลดลดลดข้อมูลส่วนตัว ไฟล์งาน รูปภาพ การใช้งานสมาร์ตโฟน แท็บเล็ต และคอมพิวเตอร์ โดยระบบต่าง ๆ ของอินเทอร์เน็ตจะบันทึกข้อมูลของผู้ใช้งาน เช่น ชื่อ และข้อมูลส่วนตัว วันเดินปีเกิด ตำแหน่งงาน ผลงาน ข้อมูลการศึกษา ประวัติส่วนตัว ของผู้ใช้งาน ร่องรอยดิจิทัล สามารถบอกให้ผู้อื่นทราบถึงสิ่งที่เราชอบ

สิ่งที่สนใจ และสิ่งที่เราอยากทำ จึงเหมือนสมุดบันทึกที่สะท้อนให้เห็นถึงกิจกรรมออนไลน์ของผู้ใช้งานร่องรอยดิจิทัล มี 2 ประเภทคือ (https://www.scimath.org/article-technology/item/10617-digital-footprint)

1. ร่องรอยดิจิทัล ที่ผู้ใช้เจตนาบันทึก (Active Digital Footprints) ร่องรอยดิจิทัล ของผู้ใช้งานที่เจตนาบันทึกไว้ในโลกออนไลน์ ข้อมูลที่เราตั้งใจเปิดเผยโดยที่รู้ตัว เช่น อีเมล เบอร์โทร ชื่อโปรไฟล์ เฟซบุ๊ก หรือสิ่งที่เราตั้งใจโพสต์ลงในโซเชียลมีเดีย เช่น สิ่งที่เราพูดหรือโพสต์ รูปที่เราเคยลง สิ่งที่เรากดไลก์ รีทวิต หรือแชร์ ที่ตั้งสถานที่ที่เราอยู่หรือเคยไป

2. ร่องรอยดิจิทัล ที่ผู้ใช้ไม่เจตนาบันทึก (Passive Digital Footprints) ร่องรอยดิจิทัลของผู้ใช้งานที่ไม่มีเจตนาบันทึกเอาไว้ในโลกออนไลน์ หรือข้อมูลแบบที่ไม่ได้ตั้งใจหรือไม่ได้รู้ตัว เช่น IP Address หรือ Search History ต่าง ๆ ที่เราถูกจัดเก็บเอาไว้ สิ่งที่เราเคยคลิกเข้าไป การซื้อสินค้าออนไลน์ของเรา การเปิดระบบ GPS เป็นต้น

ประเภทของภัยคุกคามทางไซเบอร์

1. Malicious Software หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย ดังนั้นผู้ใช้งานคอมพิวเตอร์ทุกคนควรรู้ลักษณะและพฤติกรรมการทำการทำงานของมัลแวร์ในแต่ละประเภท

- Virus มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่นๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น
- Worm สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่นๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์ของผู้ใช้
- Trojan หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริงๆแล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย
- Backdoor เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว
- Spyware แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน , รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย
- Ransomware ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้จากนั้นก็จะส่งข้อความ "เรียกค่าไถ่" เพื่อแลกกับการถอดรหัสเพื่อกู้ขันมา
- Scareware เป็นโปรแกรมที่ถูกเขียนขึ้น เพื่อทำให้ผู้ใช้งานคอมพิวเตอร์เข้าใจว่า เครื่องคอมพิวเตอร์ของตัวเองมีไวรัส โดยมักมีการแจ้งเตือนว่าพบไวรัสในเครื่องคอมพิวเตอร์ ทำให้ผู้ใช้หลงเชื่อให้ข้อมูลบัตรเครดิต ซื้อหรือดาวน์โหลดซอฟต์แวร์ เพื่อกำจัดไวรัสนั้น ซึ่งซอฟต์แวร์ดังกล่าวเป็นซอฟต์แวร์ปลอมที่ส่งผลให้เกิดอันตรายต่อความปลอดภัยของข้อมูลส่วนตัวและคอมพิวเตอร์
- Adware หมายถึงแพ็กเกจซอฟต์แวร์ใดๆ ที่สามารถทำงาน แสดง หรือดาวน์โหลดสื่อโฆษณาโดยอัตโนมัติไปยังคอมพิวเตอร์ที่ได้รับการติดตั้งซอฟต์แวร์ชนิดนี้ไว้ หรือขณะที่โปรแกรมประยุกต์กำลังเรียกใช้ ซอฟต์แวร์โฆษณาบางประเภทเป็นซอฟต์แวร์สอดแนม (spyware)

2. DoS Attack (denial-of-service attack) หรือ distributed denial-of-service (DDoS) attack การโจมตีโดยปฏิเสธการให้บริการ เป็นความพยายามทำให้เครื่องหรือทรัพยากรเครือข่ายสำหรับผู้ใช้เป้าหมายใช้บริการไม่ได้ เช่น ขัดขวางหรือชะลอบริการของแม่ข่ายที่เชื่อมโยงกับอินเทอร์เน็ตอย่างชั่วคราวหรือถาวร อาชญากรผู้โจมตีมักมุ่งเป้าไปยังเว็บไซต์หรือบริการซึ่งตั้งอยู่ในเว็บเซิร์ฟเวอร์ที่มีการเข้าชมสูงอย่างเช่น ธนาคาร เกตเวย์ชำระบัตรเครดิต โดยมีแรงจูงใจเบื้องหลังเป็นการแก้แค้นการแบล็กเมล์ หรือการเคลื่อนไหวทางการเมือง เป็นต้น

3. Phishing คือ กลลวงที่แอบผลทางอินเทอร์เน็ตซึ่งมักมาในรูปแบบของการปลอมแปลงอีเมลงอีเมลหรือข้อความที่สร้างขึ้นเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนตัวต่างๆPhishing สามารถทำได้โดยการส่งอีเมล หรือข้อข้อความที่อ้างว่ามาจากองค์กรต่างๆ ที่ท่านติดต่อด้วยเช่น บริษัทให้บริการอินเทอร์เน็ตหรือธนาคาร โดยส่งข้อความเพื่อขอให้ท่าน "อัปเดต" หรือ "ยืนยัน"ข้อมูลบัญชีของท่าน หากท่านไม่ตอบกลับอีเมลดังกล่าว อาจก่อให้เกิดผลเสียตามมาได้

5. การรู้เท่าทันสื่อและสารสนเทศ (Media and Information Literacy)

MIL (Media and Information Literacy) หมายถึง ความรู้และความเข้าใจวิธีการทำงานของสื่อ วิธีที่สื่อสร้างความหมาย วิธีใช้สื่อ และวิธีประเมินข้อมูลข่าวสารที่สื่อนำเสนอ นอกจากนี้ ยังมีความหมายโดยนัยถึงความรู้และความเข้าใจในคุณค่าของบุคคลและทางสังคม หน้าที่รับผิดชอบที่เกี่ยวข้องกับการใช้เทคโนโลยีและสารสนเทศอย่างมีจริยธรรม ตลอดจนการมีส่วนร่วมในบทสนทนาเกี่ยวกับประชาธิปไตยและวัฒนธรรม

M การรู้เท่าทันสื่อ (Media Literacy) สมรรถนะในการใช้สื่อต่างๆ รวมถึงการวิเคราะห์ และเข้าใจในรูปแบบของสื่อ และเทคนิคต่างๆ ที่สื่อใช้ในการสร้าง ผลกระทบต่อผู้รับสื่อและความสามารถในการอ่านวิเคราะห์ประเมิน และสร้างสื่อในหลากหลายรูปแบบได้

I การรู้เท่าทันสารสนเทศ (Information Literacy) สมรรถนะในการประเมิน เลือกใช้และสื่อสารข้อมูลได้อย่างมีประสิทธิภาพในหลากหลายรูปแบบ และรวมถึงความเข้าใจข้อมูลสารสนเทศต่างๆ ในความหมายเชิงจริยธรรม

D การรู้เท่าทันดิจิทัล (Digital Literacy) สมรรถนะในการใช้เทคโนโลยีดิจิทัล เครื่องมือสื่อสารเครือข่ายต่างๆ เพื่อค้นหาข้อมูล (เข้าถึง) ประมวลผล (เข้าใจ) และสร้างสรรค์ข้อมูล (ประยุกต์ใช้) ได้หลากหลายรูปแบบ

ทำความรู้จัก Data และ Information คืออะไร

Data หรือข้อมูล คือ ข้อเท็จจริงที่ยังไม่ได้รับการจัดการ จัดรูปแบบ หรือผ่านกระบวนการจัดการข้อมูล ซึ่งข้อมูลเหล่านี้คือ ข้อมูลดิบ หรือที่เรียกว่า Raw Data โดยข้อมูลที่ว่านั้นมีหลากหลาย ทั้งข้อความ ตัวเลข ภาพ เอกสาร วิดีโอ และข้อมูลอื่น ๆ ทั้งนี้ ข้อมูลที่ได้มาจะเป็นข้อเท็จจริงทั้งหมด ไม่ว่าจะเป็นการสังเกต การวัด ตัวเลขต่าง ๆ เช่น ชาย สีขาว หรือ 13 ซึ่งข้อมูลส่วนนี้เราไม่สามารถทราบได้เลยว่า ข้อมูลดิบดังกล่าวจะใช้สื่อในรูปแบบไหน หรือมีคำอธิบายเป็นอย่างไร จนกว่าจะผ่านขั้นตอนการจัดการข้อมูลก่อนนั่นเอง

Information หรือ สารสนเทศ คือ ข้อมูลที่ผ่านการจัดการ การจัดเรียง การกลั่นกรอง การกำหนดรูปแบบของข้อมูล (Data) โดยจะเป็นชุดข้อมูลหรือที่เรียกว่า Data Collection ที่ประกอบรวมกับบริบท Context หรือผ่านการให้ความหมายมาเรียบร้อยแล้ว และสามารถนำข้อมูลเหล่านี้ไปใช้ประโยชน์ได้ โดย Information หรือ สารสนเทศ อาจถูกนำเสนอในรูปแบบของรายงาน สรุปผลข้อมูล เรียกง่าย ๆ ว่า สารสนเทศ คือ ผลลัพธ์ของข้อมูลที่ผ่านกระบวนการจัดการข้อมูลแล้ว

6. แนวปฏิบัติในสังคมดิจิทัล (Digital Etiquette)

- Network Etiquette หมายถึง จรรยามารยาทของการอยู่ร่วมกันในสังคมอินเทอร์เน็ต หรือ โลกดิจิทัลซึ่งเป็นพื้นที่ที่เปิดโอกาสให้ผู้คนเข้ามาแลกเปลี่ยน สื่อสารและทำกิจกรรมรวม กัน ทั้งในชุมชนใหญ่หรือโลกบนอินเทอร์เน็ต ก็ไม่ต่างจากสังคมบนโลกแห่งความเป็นจริง ซึ่งจำเป็นต้องมีกฎ กติกาเพื่อ ใช้เป็นกลไกสำหรับการกำกับดูแลพฤติกรรมและการปฏิสัมพันธ์ของสมาชิก

มารยาทเน็ต คือ ชุดวิธีประพฤติตนที่เหมาะสมเมื่อคุณใช้อินเทอร์เน็ต

1. “อย่าลืมว่าคุณกำลังติดต่อกับคนที่มีตัวตนจริง ๆ” ก่อนส่งอีเมล หรือโพสต์ข้อความอะไรบนอินเทอร์เน็ตคุณต้องถามตัวเองว่า ถ้าเจอกันต่อหน้าคุณจะพูดแบบนี้กับเขาหรือไม่ ถ้าคำตอบคือไม่ ก็จงแก้ไขข้อความนั้นแล้วอ่านใหม่อีกครั้ง ทำแบบนี้ซ้ำๆ จนรู้สึกว่าไม่ลำบากใจที่จะพูดแบบนี้กับใครแล้วจึงค่อยส่ง
2. “การสื่อสารออนไลน์ให้ยึดมาตรฐานความประพฤติเดียวกับการสื่อสารในชีวิตจริง” ในชีวิตจริง คนส่วนใหญ่มักจะเคารพกฎหมาย เพราะกลัวโดนจับ แต่ในโลกอินเทอร์เน็ต โอกาสถูกจับมีน้อย ก็เลยปฏิบัติต่อกันโดยมีมาตรฐานทางศีลธรรมต่ำกว่าในโลกจริง ถ้าอยากทำอะไรผิดกฎหมายในไซเบอร์สเปซ สิ่งที่คุณกำลังจะทำนั้นก็น่าจะผิดด้วย
3. “รู้ว่าคุณอยู่ที่ไหนในไซเบอร์สเปซ” การกระทำอะไรก็ตามอาจเป็นเรื่องยอมรับได้ในที่แห่งหนึ่ง แต่ถ้าเป็นที่แห่งอื่นๆ อาจจะไม่ใช่ลองใช้เวลาสักพักสังเกตการณ์ก่อนว่า ที่นั่นเขาคุยอะไรกัน ปฏิบัติต่อกันอย่างไร หรือเข้าไปอ่านข้อความเก่าๆ จากนั้นค่อยเข้าไปมีส่วนร่วมกับเขา
4. “เคารพเวลาและการใช้แบนด์วิธ” ปัจจุบันดูเหมือนคนจะมีเวลาน้อยลงกว่าที่เคยเป็นมามากนัก เมื่อคุณส่งอีเมลหรือโพสต์ข้อความลงเน็ต รู้ไว้ว่าคุณกำลังทำให้คนอื่นเสียเวลามาอ่าน ดังนั้นเป็นความรับผิดชอบที่คุณควรแน่ใจก่อนส่ง ว่าข้อความหรืออีเมลนั้นไม่ทำให้ผู้รับเสียเวลา
5. “สำหรับกระดานสนทนา” ผู้ที่เข้ามาอ่านกระดานแบบนี้ส่วนใหญ่นั่งแช่หน้าจอคอมพิวเตอร์นานเกินไปอยู่แล้ว ไม่มีใครชอบหรอกถ้าต้องเสียเวลาทำทั้งหมดนั้นแล้วพบว่าไม่เห็นจะคุ้มค่าเวลาที่เสียไปเลย หากจะส่งข้อมูลอะไรไปให้ใคร ลองถามตัวเองดูก่อนว่าเขาจำเป็นจะต้องรู้เรื่องในอีเมลนั้นหรือไม่ ถ้าไม่ ก็อย่าส่ง ถ้าอาจจะอยากรู้ก็ทบทวนก่อนส่ง
6. “ทำให้ตัวเองดูดีเวลาออนไลน์” โลกอินเทอร์เน็ตก็เหมือนโลกจริง คนที่สื่อสารกันในนั้นอยากให้คนอื่นชอบ แต่คุณไม่ต้องถูกตัดสินด้วย สีผิว, สีตา, สีผม, น้ำหนัก, อายุ หรือการแต่งตัวของคุณ คุณจะถูกตัดสินผ่านคุณภาพของสิ่งที่คุณเขียน ดังนั้น การสะกดคำให้ถูกและเขียนให้ตรงตามหลักไวยากรณ์จึงเป็นเรื่องสำคัญ ควรรู้ว่าตัวเองกำลังพูดอะไรอยู่ และพูดอย่างมีเหตุมีผล
7. “แบ่งปันความรู้ของผู้เชี่ยวชาญ” จุดแข็งของไซเบอร์สเปซ คือ มีผู้เชี่ยวชาญมากมายที่อ่านคำถามบนอินเทอร์เน็ต และถึงแม้ว่าจะมีส่วนน้อยมากในจำนวนนั้นที่ตอบคำถาม ความรู้โดยรวมของโลกก็เพิ่มขึ้นอยู่ดี แม้ว่ามารยาทเน็ตจะมีข้อห้ามยาวเหยียด คุณก็มีความรู้ที่เป็นประโยชน์กับคนอื่น อย่ากลัวที่จะแบ่งปันในสิ่งที่คุณรู้
8. “ช่วยกันควบคุมสงครามการใส่อารมณ์” เวลาที่ต้องการแสดงความคิดเห็นอย่างรุนแรง ควรรู้จักยับยั้งชั่งใจหรือพยายามควบคุมอารมณ์ให้มาก
9. “เคารพความเป็นส่วนตัวของผู้อื่น” คุณไม่ควรไปเปิดอ่านอีเมลของคนอื่น การไม่เคารพความเป็นส่วนตัวของผู้อื่นไม่ได้เป็นแค่มารยาทเน็ตที่เลวทราม เท่านั้น มันยังอาจทำให้คุณเสียงานด้วย “อย่าใช้อำนาจในทางไม่สร้างสรรค์” การรู้มากกว่าคนอื่นหรือมีอำนาจมากกว่า ไม่ได้แปลว่าคุณมีสิทธิที่จะเอาเปรียบคนอื่นได้ เช่น ผู้ดูแลระบบไม่ควรอ่านอีเมลส่วนตัวของคนอื่น

10. “ให้อภัยในความผิดพลาดของผู้อื่น” ทุกคนเคยเป็นมือใหม่มาก่อน บางคนจึงทำผิดพลาดในแง่มารยาทเน็ต จงใจเย็นเข้าไว้ ถ้าคุณตัดสินใจจะบอกคนที่ทำผิดมารยาทเน็ต ก็จงบอกอย่างสุภาพและเป็นส่วนตัว ดีกว่าไปป่าวประกาศให้คนอื่นรับรู้ด้วย จงให้โอกาสในความไม่รู้ของคนอื่น การประณามว่าผู้อื่นไม่มีมารยาทตรงๆ ก็มักจะเป็นตัวอย่างของมารยาทที่ไม่ดีเช่นกัน

- **การกลั่นแกล้งบนโลกออนไลน์ (Cyberbullying)**

คือการรังแกผู้อื่นผ่านทางโลกออนไลน์ โดยการรังแกในที่นี้เป็นได้ทั้ง การด่าทอ กล่าวหา ใช้ถ้อยคำเสียดสี ต่อว่าผู้อื่นโดยเป็นการแกล้งที่เจาะจงบุคคลเป้าหมาย และมีแนวโน้มว่าจะเป็นการรังแกที่ต่อเนื่อง ไม่ใช่แค่ครั้งเดียวจบ

7. สุขภาพดียุคดิจิทัล (Digital Health)

เรียนรู้อันตรายและผลกระทบด้านสุขภาพในแง่มุมต่าง ๆ ไม่ว่าจะเป็นด้านสุขภาพกาย สุขภาพจิต โรคที่เกิดขึ้น รวมถึงความสัมพันธ์และผลกระทบต่อเยาวชน การใช้อินเทอร์เน็ตและสื่อดิจิทัล เพื่อป้องกันหลีกเลี่ยง ลดผลกระทบ จนถึงวิธีการรักษาเบื้องต้น ทั้งต่อตนเอง และคนใกล้ตัว เพื่อให้สามารถใช้ชีวิตอย่างมีความสุขในยุคดิจิทัลได้

8. กฎหมายดิจิทัล (Digital Law)

เรียนรู้กฎหมายที่เกี่ยวข้องกับทรัพย์สินทางปัญญา และกฎหมายที่เกี่ยวข้องกับเศรษฐกิจดิจิทัล เพื่อให้ระบุได้ว่าการกระทำใดเป็นความผิดที่เกี่ยวกับกฎหมายดิจิทัล ทราบถึงโทษของการกระทำความผิด มีแนวทางป้องกันการกระทำความผิดที่เกี่ยวกับกฎหมายดิจิทัล

- **กฎหมายที่เกี่ยวข้องกับทรัพย์สินทางปัญญา**

ทรัพย์สินทางปัญญา หมายถึง ผลงานอันเกิดจากการประดิษฐ์ คิดค้น หรือสร้างสรรค์ของมนุษย์ ซึ่งเน้นที่ผลผลิตของสติปัญญาและความชำนาญ โดยไม่คำนึงถึงชนิดของการสร้างสรรค์หรือวิธีในการแสดงออก เช่น สินค้าต่าง ๆ การบริการ กรรมวิธีการผลิตทางอุตสาหกรรม เป็นต้น
ทรัพย์สินทางปัญญามีกี่ประเภทในทางสากล ทรัพย์สินทางปัญญาแบ่งเป็น 2 ประเภท ได้แก่ ทรัพย์สินทางอุตสาหกรรม (Industrial Property) และ ลิขสิทธิ์ (Copyright)

- **ทรัพย์สินทางอุตสาหกรรม (Industrial Property)**

ทรัพย์สินทางอุตสาหกรรม หมายถึง ความคิดสร้างสรรค์ของมนุษย์ที่เกี่ยวกับสินค้าอุตสาหกรรมต่าง ๆ ที่ได้พัฒนาหรือคิดค้นขึ้นใหม่ นอกจากนี้ยังรวมถึงการออกแบบผลิตภัณฑ์เครื่องหมายการค้า ชื่อและถิ่นที่อยู่ทางการค้า โดยรวมถึงแหล่งกำเนิดและการป้องกันการแข่งขันทางการค้าที่ไม่เป็นธรรม ทรัพย์สินทางอุตสาหกรรม ได้แก่ สิทธิบัตร (Patent) , แบบผังภูมิของวงจรรวม (Layout-Designs of Integrated Circuit), เครื่องหมายการค้า (Trademark) ,ความลับทางการค้า (Trade Secrets) , ชื่อทางการค้า (Trade Name) และ สิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication)

- **ลิขสิทธิ์ (Copyright)**

ลิขสิทธิ์ หมายถึง สิทธิแต่เพียงผู้เดียวของผู้สร้างสรรค์ที่จะกระทำการใด ๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้นตามประเภทลิขสิทธิ์ที่กฎหมายกำหนด ได้แก่ งานวรรณกรรม นาฏกรรม ศิลปกรรม ดนตรีกรรม โสตทัศนวัสดุ ภาพยนตร์ สิ่งบันทึกเสียง งานแพร่เสียง แพร่ภาพ หรืองานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ ไม่ว่างานดังกล่าวจะแสดงออกโดยวิธีหรือรูปแบบทั้งโดยจับต้องได้และจับต้องไม่ได้ นอกจากนั้นกฎหมายลิขสิทธิ์ยังให้ความคุ้มครองถึงสิทธิของนักแสดงด้วย อย่างไรก็ตาม การคุ้มครอง

ลิขสิทธิ์ ไม่ครอบคลุมถึงความคิดหรือขั้นตอน กรรมวิธีหรือระบบ วิธีใช้หรือทำงาน แนวความคิด หลักการ การค้นพบ หรือทฤษฎีทางวิทยาศาสตร์ หรือคณิตศาสตร์

- **สิทธิบัตร (Patent)**

สิทธิบัตร คือ หนังสือสำคัญที่รัฐออกให้เพื่อคุ้มครองการประดิษฐ์ (Invention) หรือ การออกแบบผลิตภัณฑ์ (Industrial Design) ที่มีลักษณะตามที่กฎหมายกำหนด ได้แก่ สิทธิบัตรการประดิษฐ์ (Invention Patent) สิทธิบัตรการออกแบบผลิตภัณฑ์ (Design Patent) และอนุสิทธิบัตร (Petty Patent) ซึ่งผู้ทรงสิทธิบัตรหรืออนุสิทธิบัตร มีสิทธิเด็ดขาด หรือ สิทธิแต่เพียงผู้เดียวในการแสวงหาผลประโยชน์จากการประดิษฐ์ หรือการออกแบบผลิตภัณฑ์ที่ได้รับสิทธิบัตร หรือ อนุสิทธิบัตรนั้น ภายในระยะเวลาตามที่กฎหมายกำหนดประเภทของสิทธิบัตร มี 3 ประเภท ได้แก่

– สิทธิบัตรการประดิษฐ์ (Invention Patent) หมายถึง การให้ความคุ้มครองการคิดค้นเกี่ยวกับลักษณะองค์ประกอบโครงสร้าง หรือกลไกของผลิตภัณฑ์ รวมทั้งกรรมวิธีในการผลิต การเก็บรักษา หรือการปรับปรุงคุณภาพของผลิตภัณฑ์

– สิทธิบัตรการออกแบบผลิตภัณฑ์ (Design Patent) หมายถึง การให้ความคุ้มครองความคิดสร้างสรรค์ที่เกี่ยวกับรูปร่างลักษณะภายนอกของผลิตภัณฑ์ องค์ประกอบของลวดลาย หรือสีของผลิตภัณฑ์ ซึ่งสามารถใช้เป็นแบบสำหรับผลิตภัณฑ์อุตสาหกรรม รวมทั้งหัตถกรรมได้ และแตกต่างไปจากเดิม

– อนุสิทธิบัตร (Petty Patent) คือ การให้ความคุ้มครองการประดิษฐ์จากความคิดสร้างสรรค์ที่มีระดับการพัฒนาเทคโนโลยีไม่สูงมาก โดยอาจเป็นการประดิษฐ์คิดค้นขึ้นใหม่ หรือปรับปรุงจากการประดิษฐ์ที่มีอยู่ก่อนเพียงเล็กน้อย

- อายุการให้ความคุ้มครองสิทธิบัตร

สิทธิบัตรการประดิษฐ์ มีอายุ 20 ปี นับแต่วันขอรับสิทธิบัตรสิทธิบัตรการออกแบบผลิตภัณฑ์ มีอายุ 10 ปี นับแต่วันขอรับสิทธิบัตร (https://www.en.kku.ac.th/web/ความรู้เบื้องต้นด้านทรัพย์สินทางปัญญา)

- กฎหมายดิจิทัลในประเทศไทย

1.กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562 เป็นกฎหมายกลางที่รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ให้มีผลผูกพันและใช้บังคับได้ตามกฎหมาย ซึ่งได้ประกาศเป็นกฎหมายแล้ว เมื่อวันที่ 22 พฤษภาคม 2562 และมีผลใช้บังคับเมื่อวันที่ 23 พฤษภาคม 2562
ขอบเขตการใช้บังคับ มีดังนี้

- ธุรกรรมทางแพ่งและพาณิชย์ เช่น การทำสัญญากู้ยืมเงินทางอิเล็กทรอนิกส์ การปลดหนี้เงินกู้ทางอิเล็กทรอนิกส์ แต่ไม่ใช้กับธุรกรรมเกี่ยวกับครอบครัวและธุรกรรมเกี่ยวกับมรดก
- ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ เช่น คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ เช่น การยื่นภาษีทางออนไลน์ เป็นต้น

2.กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 ที่สภานิติบัญญัติแห่งชาติให้ความเห็นชอบเมื่อเดือนธันวาคม 2559 และได้ประกาศลงราชกิจจานุเบกษา เมื่อวันที่ 24 มกราคม 2560 มีผลบังคับใช้แล้วในวันที่ 24 พ.ค. 2560 ซึ่งมีสาระสำคัญ เช่น การฝากร้านใน Facebook และ Instagram ถือว่าเป็นสแปม มีโทษปรับ 200,000 บาท ส่ง SMS โฆษณาโดยไม่รับความยินยอมให้ผู้รับสามารถ

ปฏิเสธข้อมูลนั้นได้ ถือว่าเป็นสแปม มีโทษปรับ 200,000 บาท ส่ง Email ขายของ ถือว่าเป็นสแปม มีโทษปรับ 200,000 บาท

3.กฎหมายคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ PDPA

PDPA ย่อมาจาก Personal Data Protection เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคลเพื่อรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และปัจจุบันได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565

การคุ้มครองข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ทั้งทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล, เลขประจำตัวประชาชน, เบอร์โทรศัพท์มือถือ, อาชีพ, ข้อมูลการศึกษา, ข้อมูลการเงิน, รูปถ่าย เป็นต้น

4.กฎหมายความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศที่กระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ซึ่งมีบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม พ.ศ. 2562