



บันทึกข้อความ

ส่วนราชการ กลุ่มวิเคราะห์สภาพการใช้ที่ดิน กองนโยบายและแผนการใช้ที่ดิน โทร. ๒๑๘๕

ที่ กษ ๐๘๓๗.๐๒/๑๗๐

วันที่ ๑๓ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอส่งสรุปรายงานการอบรม ปิงบประมาณ ๒๕๖๙ ครั้งที่ ๑

เรียน ผอ. กลุ่มวิเคราะห์สภาพการใช้ที่ดิน

ด้วยข้าพเจ้า นางสาวจิรัชยา คงทน นักวิชาการเกษตรชำนาญการพิเศษ กลุ่มวิเคราะห์สภาพการใช้ที่ดิน กองนโยบายและแผนการใช้ที่ดิน ได้เข้ารับการอบรม จำนวน ๒ เรื่อง ดังนี้

๑. การอบรมผ่านสื่ออิเล็กทรอนิกส์ (TDGA e-Learning) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หลักสูตร ความรู้และความเข้าใจเกี่ยวกับปัญญาประดิษฐ์ (Artificial Intelligence) ในวันที่ ๔ กุมภาพันธ์ ๒๕๖๙

๒. การอบรมผ่านสื่ออิเล็กทรอนิกส์ (TDGA e-Learning) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หลักสูตร ความฉลาดทางดิจิทัล (Digital Intelligence) ในระหว่างวันที่ ๖ - ๑๐ กุมภาพันธ์ ๒๕๖๙

ในการนี้ ได้ดำเนินการสรุปรายงานการอบรม เสร็จเรียบร้อยแล้ว จำนวน ๑ เรื่อง จึงขอส่งสรุปรายงานการอบรม ตามเอกสารที่ได้แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ และแจ้ง ผอ.กนผ. ลงนามในหนังสือที่ได้แนบมาพร้อมนี้

(นางสาวจิรัชยา คงทน)

นักวิชาการเกษตรชำนาญการพิเศษ

เรียน ผอ.กนผ.

เพื่อโปรดทราบ และลงนามในเอกสารที่แนบ

(นางสาวอมรรัตน์ สระเพชร)

นักวิชาการเกษตรชำนาญการพิเศษ

ผู้อำนวยการกลุ่มวิเคราะห์สภาพการใช้ที่ดิน

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

ส่วนที่ ๑ ข้อมูลทั่วไป
ชื่อ นางสาวจิรัชยา นามสกุล คงทน ✓ ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ กลุ่ม/ฝ่าย กลุ่มวิเคราะห์สภาพการใช้ที่ดิน หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ ความฉลาดทางด้านดิจิทัล (Digital Intelligence) สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ ระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (TDGA e-Learning) ✓ หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ตั้งแต่วันที่ ๖ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙ ถึงวันที่ ๑๐ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙ เพื่อ <input checked="" type="checkbox"/> อบรม <input type="checkbox"/> สัมมนา <input type="checkbox"/> อื่นๆ ระบุ _____
ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้
๒.๑ รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/สัมมนา/พัฒนาความรู้ฯ การอบรมครั้งนี้มีเนื้อหาสำคัญเกี่ยวกับความฉลาดทางดิจิทัล การใช้เทคโนโลยีดิจิทัลและสื่อ โดยมีหัวข้อในการอบรมดังนี้ บทนำ ความฉลาดทางดิจิทัล เป็นความสามารถในการใช้เทคโนโลยีดิจิทัล และข้อมูลในการตัดสินใจ และแก้ปัญหา โดยใช้ความรู้ ทักษะ ด้านเทคโนโลยีในการวิเคราะห์ข้อมูล และการประมวลผลข้อมูล ความฉลาดทางด้านดิจิทัล เป็นกรอบแนวความคิดทางด้านเทคนิค ความรู้ ความเข้าใจ และความคิดทางสังคม ที่มีพื้นฐานอยู่บนค่านิยมทางศีลธรรมที่ช่วยให้บุคคลเผชิญหน้ากับความท้าทายทางด้านดิจิทัล ความฉลาดทางด้านดิจิทัลมี ๓ ระดับ ๘ ด้าน และ ๒๕ สมรรถนะ ที่ประกอบไปด้วย ความรู้ ทักษะ ทักษะคิด และค่านิยม จะพุดถึงทักษะ ๘ ด้าน ในระดับพลเมืองดิจิทัล ซึ่งเป็นความสามารถในการใช้เทคโนโลยีดิจิทัลและสื่อ ในรูปแบบที่ปลอดภัย รับผิดชอบ มีจริยธรรม ดังนี้ ๑. ทักษะในการรักษาอัตลักษณ์ที่ดีของตนเอง (Digital Citizen Identity) เป็นความสามารถในการสร้างและบริหารจัดการอัตลักษณ์ที่ดีของตนเองไว้ได้อย่างดีในโลกออนไลน์ และโลกความจริง ๒. ทักษะการคิดวิเคราะห์ มีวิจารณญาณที่ดี (Critical Thinking) เป็นความสามารถในการวิเคราะห์ แยกแยะระหว่างข้อมูลที่ถูกต้องและข้อมูลที่ผิด ข้อมูลที่มีเนื้อหาดีและข้อมูลที่เข้าข่ายอันตราย ข้อมูลติดต่อทางออนไลน์ที่น่าตั้งข้อสงสัยและน่าเชื่อถือได้ ๓. ทักษะในการรักษาความปลอดภัยของตนเองในโลกไซเบอร์ (Cyber Security Management) เป็นความสามารถในการป้องกันข้อมูลด้วยการสร้างสรรค์ระบบความปลอดภัยที่เข้มแข็ง และป้องกันการโจรกรรมข้อมูลหรือการโจมตีทางออนไลน์ได้ ซึ่งมีวัตถุประสงค์เพื่อ ๑) การรักษาความเป็นส่วนตัวและความลับ ๒) เพื่อ

ป้องกันการขโมยอัตลักษณ์ ๓) เพื่อป้องกันการโจรกรรมของข้อมูล ๔) เพื่อป้องกันความเสียหายของข้อมูลและอุปกรณ์

๔. ทักษะในการรักษาข้อมูลส่วนตัว (Privacy Management) เป็นการมีดุลพินิจในการบริหารจัดการข้อมูลส่วนตัว โดยเฉพาะการแชร์ข้อมูลออนไลน์ เพื่อป้องกันความเป็นส่วนตัวทั้งของตนเองและผู้อื่น

๕. ทักษะในการจัดสรรเวลาหน้าจอ (Screen Time Management) เป็นความสามารถในการบริหารเวลาในการใช้อุปกรณ์ยุคดิจิทัล รวมไปถึงการควบคุมเพื่อให้เกิดสมดุลระหว่าง โลกออนไลน์ และโลกภายนอก

๖. ทักษะในการบริหารจัดการข้อมูลที่ใช้งานมีการทิ้งไว้บนโลกออนไลน์ (Digital footprints) เป็นความสามารถในการเข้าใจธรรมชาติของการใช้ชีวิตในโลกดิจิทัล ที่จะหลงเหลือร่องรอยข้อมูลทิ้งไว้เสมอ รวมไปถึงเข้าใจผลลัพธ์ที่อาจเกิดขึ้น เพื่อการดูแลสิ่งเหล่านี้อย่างมีความรับผิดชอบ

๗. ทักษะในการรับมือกับการกลั่นแกล้งบนโลกไซเบอร์ (Cyberbullying Management) เป็นความสามารถในการรับรู้ และการรับมือการคุกคาม ช่มชู้ บนโลกออนไลน์ได้อย่างชาญฉลาด

๘. ทักษะการใช้เทคโนโลยีอย่างมีจริยธรรม (Digital Empathy) เป็นการมีดุลพินิจในการบริหารจัดการข้อมูลส่วนตัว โดยเฉพาะการแชร์ข้อมูลออนไลน์ เพื่อป้องกันความเป็นส่วนตัวของทั้งตนเองและผู้อื่น คิดก่อนโพสต์ ตั้งคำถามก่อนเสมอว่า ควรจะโพสต์หรือไม่

๑. อัตลักษณ์ดิจิทัล (Digital Identity)

๑.๑ โลกดิจิทัล (Digital World) คือโลกเสมือนที่ถูกสร้างขึ้นคู่ขนานกับโลกความจริง ซึ่งมีพื้นที่ ผู้คน เครื่องมือ ทรัพยากร กิจกรรม คล้ายกับโลกของความจริง พื้นที่ในโลกดิจิทัลถูกสร้างขึ้นมาจากอุปกรณ์อิเล็กทรอนิกส์ ที่สามารถกำหนดกิจกรรมต่าง ๆ ได้เสมือนกับโลกความเป็นจริง เป็นพื้นที่พูดคุยแลกเปลี่ยนประสบการณ์ พื้นที่ในการขายสินค้า ทำธุรกรรม ร้านค้าออนไลน์ ธนาคารออนไลน์ ใช้เฉพาะสมาชิก หรือพลเมืองดิจิทัลเท่านั้น

เปรียบเทียบโลกดิจิทัล กับ โลกความจริง

๑) การเข้าถึงสื่อที่ต้องการ

โลกดิจิทัล : เข้าถึงได้สะดวกกว่าด้วยอุปกรณ์พกพา โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ เราสามารถค้นหาข้อมูล นำสื่อมาใช้ได้ง่าย สะดวกทุกที่ทุกเวลา

โลกความจริง : มีข้อจำกัดการเข้าถึง ต้องเดินทางไปยังที่เก็บข้อมูล ต้องรอข่าวสาร มีวัน เวลาในการให้บริการ

๒) การพูดคุยติดต่อ

โลกดิจิทัล : ทำได้อย่างรวดเร็ว ส่งข้อความในแอปพลิเคชัน หากมีเรื่องด่วนสามารถโทรด้วยภาพและเสียง

โลกความจริง : ต้องรอให้ว่างตรงกัน ต้องอยู่ในสถานที่เดียวกัน มีข้อจำกัดในการพูดคุย

๓) การเผยแพร่สื่อ เนื้อหา บอกเล่าประสบการณ์ ความรู้สึกต่าง ๆ

โลกดิจิทัล : ใช้โซเชียลมีเดียโพสต์แบ่งปันความรู้สึก การเผยแพร่รูปภาพ วิดีโอที่เป็นประโยชน์กับผู้อ่าน

โลกความจริง : อาจจำกัดการเผยแพร่ด้วยการบอกเล่า รับรู้ได้แค่บุคคลใกล้ชิด เช่น ครอบครัว เพื่อน

๔) การให้คำปรึกษา สร้างแรงบันดาลใจ

โลกดิจิทัล : ทำได้ไม่ค่อยดี เพราะอาศัยการพิมพ์ ความรู้สึกไม่สามารถถ่ายทอดได้อย่างเต็มที่

โลกความจริง : ได้เห็นหน้า มองตา สัมผัสกาย เห็นอกเห็นใจ เกิดความเข้าใจทั้งในด้านเนื้อหา และอารมณ์ได้ดีมากขึ้น

๕) การร่วมกิจกรรมที่อาศัยการปฏิบัติ

โลกดิจิทัล : อาจทำได้ในบางเรื่อง ที่ไม่ซับซ้อน

โลกความจริง : อาศัยผู้เชี่ยวชาญ หรือผู้มีประสบการณ์ จะใช้กิจกรรมที่ปฏิบัติละเอียดลออ ปรานีต เช่น เทคนิคที่ต้องอาศัยผู้เชี่ยวชาญ หรือผู้มีประสบการณ์อย่างใกล้ชิด มีประสิทธิภาพมากกว่า เช่น การฝึกทำขนมไทย การแกะสลักผักผลไม้

๖) การทำธุรกรรมของภาครัฐในบางประเภท

โลกดิจิทัล : มีการทำผ่านระบบดิจิทัล เช่น การเงิน ต้องไปทำในโลกความจริงบางส่วน เช่น การโอนที่ดิน ทำใบขับขี่ ทำบัตรประชาชน

โลกความจริง : ทำธุรกรรมได้ทุกประเภท หากเดินทางไปทำการ

มารยาทในโลกดิจิทัล

สิ่งที่ควรทำ ๑) ใส่ใจและให้เกียรติไม่ต่างจากโลกความจริง ๒) แบ่งปันสิ่งดี ๆ และสร้างสรรค์ ๓) ตรวจสอบการส่งข้อมูลให้ตรงกับกลุ่มเป้าหมาย ๔) ปฏิบัติตามกฎหมายชุมชน และโลกออนไลน์

สิ่งที่ไม่ควรทำ ๑) การแสดงความเห็นด้วยถ้อยคำที่รุนแรง ๒) แสดงอารมณ์ขันที่หมิ่นเหม่เสียดสี ๓) ส่งต่อข้อมูลที่เรไม่แน่ใจว่าเป็นความจริง ๔) ใช้โซเชียลมีเดียในการให้ร้ายผู้อื่น

จริยธรรมพลเมือง ความเข้าอกเข้าใจ การปฏิบัติที่เกิดขึ้นในสังคมพลเมืองดิจิทัลที่น่าอยู่

- ให้เกียรติและเคารพความคิดเห็น และสิทธิของผู้อื่น
- หลีกเลี่ยงการระราน ช่มชู้ หรือหยอกล้อเกินพอดี
- ขออนุญาตเมื่อทำข้อมูลผู้อื่นไปใช้
- ไตร่ตรองก่อนแชร์ หรือโพสต์ข้อมูล
- ไม่ควรแชร์หรือโพสต์ข้อมูลส่วนบุคคลมากเกินไป
- ระวังระวังในการแชร์ หรือโพสต์ข้อมูล
- หลีกเลี่ยงการแท็กภาพ หรือข้อมูลทางผู้อื่น
- ระวังการใช้ความเป็นอาวุโสในการสนทนา

สรุป โลกดิจิทัลกับโลกความจริง แตกต่างกันในเรื่องของช่องทาง เครื่องมือการสื่อสาร โลกดิจิทัลจะเน้นการใช้เครื่องมือทางอิเล็กทรอนิกส์ และระบบเครือข่ายในการติดต่อสื่อสาร ส่วนกิจกรรมต่าง ๆ บนโลกดิจิทัลจะใกล้เคียงโลกความจริง เพียงมีรูปแบบที่เปลี่ยนไป ดังนั้นอยู่ในโลกดิจิทัลอย่างปลอดภัยและมีความสุข ย่อมต้องมีมารยาทยึดหลักจริยธรรม และปฏิบัติตามกฎหมายไม่ต่างจากการใช้ชีวิตในโลกความจริง

๑.๒ อัตลักษณ์ดิจิทัล (Digital Identity) คือ ภาพลักษณ์ ตัวตน ในโลกดิจิทัลของเรา ซึ่งเกิดจากข้อมูลของเรา การเผยแพร่ข้อมูลบนโลกออนไลน์ ที่จะเป็นข้อมูลให้กับผู้อื่นจดจำเราในโลกดิจิทัล ตั้งแต่ชื่อจริง เลขบัตรประชาชน รูปภาพ เบอร์โทรศัพท์ หรือแม้แต่เสื้อผ้าที่เราใส่ในการถ่ายรูปที่เราโพสต์บนโซเชียล สถานที่ที่เราชอบไป ตลอดถึงกิจกรรมทุกอย่างที่เราทำบนโลกออนไลน์

อัตลักษณ์ทางโลกดิจิทัลที่เป็นข้อมูลเดียวกันกับโลกความเป็นจริงมี ชื่อ นามสกุล รูปภาพประจำตัว วันเดือนปีเกิด เลขบัตรประชาชน หมายเลขบัตรเครดิต หรือบัญชีธนาคาร

อัตลักษณ์ที่เกิดจากกิจกรรมบนโลกดิจิทัล ได้แก่บัญชีและรหัสผ่าน สถานที่ที่เราเช็คอิน พฤติกรรมและประวัติการค้นหา การกดถูกใจ เนื้อหา ข้อความ กลุ่มหรือสังคม เพื่อน บุคคลหรือองค์กร

ผลจากการสร้างอัตลักษณ์ดิจิทัล การสร้างอัตลักษณ์ที่ส่งผลต่อโลกความเป็นจริง ข้อมูลที่เผยแพร่ไม่สามารถลบได้จริง

- ทางบวก ผู้คนจดจำเราในทางที่ดี สร้างความสัมพันธ์ที่ดีกับคนรอบตัว เปิดโอกาสมากมาย อยู่ในสังคมดิจิทัลที่น่าอยู่

- ทางลบ ผู้คนจดจำเราในทางไม่ดี ความสัมพันธ์ที่ไม่ดี ถูกระรานในโลกดิจิทัล ถูกโจรกรรมทางดิจิทัล เสียโอกาสในหน้าที่การงาน ส่งผลกระทบต่อสภาพจิตใจ

การสร้างตัวตนใหม่มีอัตลักษณ์ดิจิทัลที่ดี

- ๑) ตระหนักอยู่เสมอว่า ทุกอย่างที่เราแชร์ หรือเผยแพร่ในโลกดิจิทัล จะอยู่ในนั้นตลอดไป
- ๒) คิดก่อนโพสต์และแชร์
- ๓) ใจเย็นให้มากที่สุดในโลกดิจิทัล
- ๔) เลิกคิดว่านี่คือ โลกจำลอง
- ๕) ทุกอย่างในโลกออนไลน์มีเจ้าของ
- ๖) อย่าให้ผู้อื่นรู้ข้อมูลของเรามากเกินไป
- ๗) ปกป้องรหัสผ่าน และเปลี่ยนบ่อย ๆ
- ๘) ตรวจสอบตัวตนของเราบนโลกดิจิทัลอยู่เสมอ

การปรับอัตลักษณ์ดิจิทัล

- ๑) ค้นหาข้อมูลของตัวเองบนโลกดิจิทัล
- ๒) การลบข้อมูลด้วยตนเอง
- ๓) การลบข้อมูลเป็นการกระทำของผู้อื่น
- ๔) เริ่มสร้างตัวตนที่ดีบนโลกดิจิทัล

อัตลักษณ์ดิจิทัล กับ ตัวตนที่แท้จริง

ข้อมูล	แนวทางปฏิบัติที่ดี
ชื่อ-นามสกุล	ควรใช้ชื่อ-นามสกุล ที่ไม่ทำให้ผู้อื่นเสียหาย และไม่ควรรู้ชื่อผู้อื่น ไม่ควรสร้างตัวตนหลอก
รูปประจำตัว	ไม่ใช่ภาพของผู้อื่นมาเป็นรูปประจำตัว หรือละเมิดทำให้ผู้อื่นเสียหาย
ข้อมูลส่วนตัว	ตั้งค่าความเป็นส่วนตัว และไม่เปิดเผยข้อมูลที่ไม่ควรเผยแพร่ เช่น เลขบัตรประชาชน
ประวัติการใช้งาน	ตรวจสอบประวัติการใช้งานบนอินเทอร์เน็ต หากประวัติเสียหายให้ทำการลบ ควรหลีกเลี่ยงการเข้าถึงเนื้อหา
เนื้อหาที่เผยแพร่	ตรวจสอบเนื้อหา ข้อความ รูปภาพที่เราได้เผยแพร่ในโลกดิจิทัล
สถานที่เช็คอิน	ตรวจสอบการใช้เครื่องมือเช็คอินบนเฟซบุ๊ก หากพบว่าไม่เหมาะสมให้ลบ
กลุ่มที่เข้าร่วม	ตรวจสอบกลุ่มที่เข้าร่วม หากมีเนื้อหาไม่เหมาะสมให้กดออกจากกลุ่ม
บุคคลที่ติดตาม	ตรวจสอบบุคคลที่รับเป็นเพื่อน หากพบว่าไม่เหมาะสมให้ลบ
ความคิดเห็น	ตรวจสอบการแสดงความคิดเห็น หากไม่เหมาะสมให้ลบ

๑.๓ ความเห็นส่วนตัวในโลกดิจิทัล (Digital Privacy)

ข้อมูลส่วนตัว (Personal Information) คือข้อมูลส่วนบุคคลที่สามารถเผยแพร่ได้ ไม่เป็นอันตราย เช่น ชื่อจริง ชื่อเล่น อายุ เพศ พี่น้อง อาหารที่ชอบ หนังสือเรื่องโปรด สัตว์เลี้ยง เป็นต้น ไม่ควรเผยแพร่ในที่สาธารณะ เนื่องจากความปลอดภัยทั้งตัวตนบนโลกดิจิทัล และโลกความเป็นจริง

การจัดการข้อมูลส่วนตัว

- ๑) ไม่เปิดเผยหรือเผยแพร่ข้อมูลที่ไม่ควรเปิดเผย
- ๒) หลีกเลี่ยงการตั้งโปรไฟล์โซเชียลมีเดียให้เป็นสาธารณะ
- ๓) จัดการอุปกรณ์ให้ปลอดภัย ไม่ว่าจะดเป็น โทรศัพท์ แท็บเล็ต หรือคอมพิวเตอร์ ควรมีระบบตั้งค่าในการเข้าถึงข้อมูล
- ๔) ทำความเข้าใจกับเงื่อนไข และข้อตกลงในการใช้โปรแกรมและแอปพลิเคชัน
- ๕) ตั้งรหัสผ่านให้มีความปลอดภัย ไม่ควรตั้งเป็นหมายเลขโทรศัพท์ เลขวันเดือนปีเกิด ควรมีอีเมลสำรองกู้คืนรหัสผ่าน

กฎหมายที่เกี่ยวข้องกับสิทธิ และความเป็นส่วนตัวในโลกดิจิทัล

PDPA (Personal Data Protection Act) คือกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยระบุให้องค์กรหรือหน่วยงานเก็บข้อมูลส่วนบุคคลของประชาชนไม่ว่าจะเป็นบริษัทเอกชน หรือหน่วยงานภาครัฐ ต้องไม่นำเอาข้อมูลส่วนตัวของเราไปใช้โดยที่เราไม่ยินยอม กฎหมายยังคุ้มครองไปถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) เช่น เชื้อชาติ เผ่าพันธุ์ ความเชื่อ ศาสนา ความเห็นทางการเมือง พฤติกรรมทางเพศ และอื่น ๆ ทั้งหมด

บทลงโทษ

- ๑) โทษทางอาญา จำคุกไม่เกิน ๑ ปี และหรือปรับสูงสุด ๑ ล้านบาท
- ๒) โทษทางแพ่ง จ่ายสินไหมไม่เกิน ๒ เท่าของสินไหมที่แท้จริง
- ๓) โทษทางปกครอง ปรับไม่เกิน ๕ ล้านบาท

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐ และ ๒๕๖๐

- ๑) ห้าม แก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย มาตรา ๙-๑๐ โทษจำคุกไม่เกิน ๒ ปี ปรับไม่เกิน ๑ แสนบาท หรือทั้งจำทั้งปรับ
- ๒) ส่งข้อมูลหรืออีเมลก่อนผู้อื่น หรือส่งอีเมลสแปม มาตรา ๑๑ โทษจำคุกไม่เกิน ๒ ปี ปรับไม่เกิน ๔ หมื่นบาท หรือทั้งจำทั้งปรับ
- ๓) นำข้อมูลที่ผิด พ.ร.บ. เข้าสู่ระบบคอมพิวเตอร์ มาตรา ๑๔ โทษจำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๖ แสนบาท หรือทั้งจำทั้งปรับ

ถ้าเป็นการกระทำความผิดต่อบุคคลใดบุคคลหนึ่ง โทษจำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๖ แสนบาท หรือทั้งจำทั้งปรับ ปัญหาการคุกคาม หรือละเมิดความเป็นส่วนตัว มีรูปแบบอะไรบ้าง และมีผลอย่างไร

- ๑) การละเมิดข้อมูลส่วนตัว จากการใช้อุปกรณ์
- ๒) การหลอกลวง ด้วยความจริงเพียงครึ่ง
- ๓) การหลอกลวงข้อมูล จากประเด็นที่อ่อนไหว
- ๔) การละเมิด หรือใช้ข้อมูลส่วนตัวที่ผิดวัตถุประสงค์ของภาคธุรกิจ

การป้องกันการคุกคามความเป็นส่วนตัวในโลกดิจิทัล

วิธีการรับมือและป้องกัน การถูกคุกคามความเป็นส่วนตัวในโลกดิจิทัล

๑) สร้างรหัสผ่านที่รัดกุม ๒) อัปเดตระบบอยู่ตลอด ๓) ตั้งค่าความปลอดภัยบนอุปกรณ์ ๔) ป้องกันอุปกรณ์ด้วยซอฟต์แวร์ป้องกันไวรัส ๕) สำรองไฟล์และข้อมูล

ควรระวังการหลอกลวงทั่วไปเหล่านี้

๑) อีเมล โทรศัพท์ และแชตหลอกลวงให้เราให้ข้อมูลส่วนตัว ๒) มีกลโกงหาข้อมูลออนไลน์ ๓) การได้รางวัลหรือกิจกรรมปลอม ๔) ร้านค้าออนไลน์ปลอม ๕) หลอกลวงว่าเกิดเหตุฉุกเฉิน

สัญญาณ และข้อสังเกตว่าการสนทนาอาจเป็นการต้มตุ๋น

๑) ผู้พูดแนะนำตัวเองเป็นพนักงานบริษัทดัง หรือหน่วยงานภาครัฐ และแจ้งสิทธิพิเศษที่ดีเกินไป หรือเรื่องด่วนที่มีความสำคัญมาก เช่น บัญชีการเงินถูกแฮก

๒) เขียนข้อความที่มีการพิมพ์ผิด หรือไวยากรณ์ไม่ดี

๓) บอกข้อมูลส่วนบุคคลที่ไม่ควรเปิดเผย เช่น รหัสผ่าน ที่อยู่แบบเต็ม รายละเอียดบัญชีธนาคารทางโทรศัพท์มือถือ หรืออีเมล

การเตือนภัยการคุกคามความเป็นส่วนตัวบนโลกดิจิทัล ในการถูกคุกคาม หรือละเมิดความเป็นส่วนตัว อาจมีการตรวจสอบผู้กระทำผิด อาจมีการดำเนินคดีตามกฎหมาย ตักเตือน หรือวิธีการอื่น เพื่อให้เขาไม่ลงมือซ้ำสร้างความตระหนักให้กับตัวเราและสมาชิกบนโลกดิจิทัล

กรณีเราถูกคุกคาม

- เมื่อพบว่าบัญชีผู้ใช้งานของเราผิดปกติ เราสามารถเข้าใช้งาน “ขอทำการพิสูจน์ตัวตน” ตั้งค่ารหัสผ่านใหม่ หรือรายงานปัญหาเมื่อถูกแฮกข้อมูลไปยังเว็บไซต์ หรือแอปพลิเคชันนั้น

- หากไม่สะดวกในการจัดการด้วยตัวเอง หรือเราไม่มีความมั่นใจ เราสามารถขอความช่วยเหลือจากเพื่อน ครอบครัว ช่วยรายงาน จัดการการละเมิดและรายงานการละเมิด หรือภัยคุกคามโลกส่วนตัวแทน

- หากพบว่าข้อมูลส่วนตัวถูกนำไปปลอมแปลงบัญชี ให้กดยางานบัญชีปลอม

- เมื่อกลับมาใช้งานได้ ให้ทำการตั้งค่าความเป็นส่วนตัวของบัญชีในระดับสูง

กรณีเมื่อพบเห็นผู้อื่นถูกคุกคาม ละเมิดความเป็นส่วนตัว

- แจ้งเจ้าตัวให้ทราบถึงเหตุการณ์เพื่อทำการตรวจสอบ

- หากตรวจสอบแล้วพบว่ามีคุกคาม แนะนำในการแก้ปัญหา

- หากแก้ไขไม่ได้ด้วยตัวเอง หรือโดยเร็ว ควรติดต่อผู้เชี่ยวชาญ หรือเป็นเรื่องสำคัญต่าง ๆ ควรเก็บหลักฐาน และแจ้งความลงบันทึกประจำวันไว้ ช่วยรายงานโพสต์ หรือบัญชีของผู้ที่ถูกคุกคาม

๒. การใช้เทคโนโลยีอย่างเหมาะสม (Digital Use)

๒.๑ การใช้เทคโนโลยีอย่างสมดุล (Balanced Use of Technology)

เวลาในการใช้หน้าจอจะมีผลต่อร่างกายและการใช้ชีวิต ๑) ปวดคอ ๒) มีผลต่อสายตา (สายตาเสีย) ๓) นั้วล็อก ๔) ถ้ามากเกินไปจะเกิดความเครียด

สมดุลเวลาหน้าจอ หลักเกณฑ์ในการจัดการสมดุลให้กับเวลาหน้าจอ

๑) โลกความเป็นจริง ให้คนเป็นเบอร์หนึ่งเสมอ

๒) มีเป้าหมายทุกครั้ง ในการใช้งานดิจิทัล

๓) ใช้ร่างกายเป็นมาตรวัด

๔) เตรียมใจให้พร้อมเพื่อเจอหน้าจอ

ผลดีในการใช้เครื่องมืออุปกรณ์เทคโนโลยี

ผลเสียในการใช้เครื่องมืออุปกรณ์เทคโนโลยี

- จอใหญ่ภาพชัด ตัวอักษรอ่านงานสบายตา
- จอตัวเล็กมองไม่ชัด มีผลต่อสายตา
- ปรับแสงหน้าจอ เพื่อให้เกิดความสบายตา
- จอสว่างจ้า มีผลทำให้สายตาเสีย
- อินเทอร์เน็ตแรง เครื่องเร็วไม่มีสะดุด
- อินเทอร์เน็ตไม่ดี ทำให้สื่อสารไม่เข้าใจ

ใช้โทรศัพท์มือถืออย่างไร ให้ใช้งานง่ายและสะดวกสบาย

๑) ขนาดหน้าจอมีความเหมาะสม ๒) ระบบการสัมผัสหน้าจอมีความสั่นไหว ๓) ฟังก์ชันการใช้งานมีความตอบโต้

ใช้โทรศัพท์มือถืออย่างไร ให้เหมาะสม ไม่ให้มีผลเสียต่อสุขภาพ

- ๑) ประกอบภาพยนตร์ในระดับสายตา ห่างจากสายตาประมาณ ๑๒ - ๑๘ นิ้ว
- ๒) ยกคอจอก คอกตั้งฉากกับลำตัว
- ๓) ควรนั่งเล่นอุปกรณ์บนเก้าอี้ ที่มีพนักพิงประมาณ ๑๐๐ องศา
- ๔) ไม่ควรเล่นติดต่อกันเกิน ๑ - ๒ ชั่วโมง
- ๕) ควรพักสายตา และข้อมูลอย่างน้อย ๕ - ๑๐ นาที ต่อชั่วโมง
- ๖) ควรปรับหน้าจอ ให้สว่างตามสภาพแสง

เนื้อหาที่น่าเชื่อถือ เป็นเนื้อหาที่รู้แหล่งที่มา นำมาปรับใช้ในชีวิตประจำวันได้ เนื้อหามีการอัปเดตเป็นปัจจุบัน ไม่สร้างผลกระทบต่อความรู้สึกและจิตใจ เป็นเนื้อหาที่ไม่สร้างความขัดแย้งรุนแรง มีความคิดแบบสุดโต่ง

สัญญาณการบอกเขตการเสพติดเนื้อหา

- เข้าไปอ่าน ดู กดโลก กดหัวใจหลาย ๆ ครั้งในหนึ่งวัน หรือเกือบทุกชั่วโมง
- หากวันไหนไม่ได้เข้าไปอ่าน กดโลก กดหัวใจ จะรู้สึกว้าวุ่นใจขาดอะไรไปสักอย่าง
- หรือทุกครั้งที่ว่า หรือมีเรื่องราวในวันนั้น แวบเข้ามาในความคิดแบบไม่ตั้งใจ เราจะอยากเข้าไปอ่าน ไปชม

เนื้อหาต่าง ๆ นั้น

ถ้าเสพติดเนื้อหา หรือเสพติดอินเทอร์เน็ตจะมีผลต่อสุขภาพจิต เกิดภาวะซึมเศร้า เสี่ยงต่อการวิตกกังวล ขาดความยับยั้งชั่งใจ รู้สึกต่อต้านสังคม

๒.๒ การเอาใจเขามาใส่ใจเราทางด้านดิจิทัล (Digital Empathy)

การเอาใจเขามาใส่ใจเราในโลกดิจิทัล

กรณีที่ ๑ คนใกล้ชิดสนิทสนม โพสต์ข้อความสิ้นหวังหมดกำลังใจในการทำงาน

ควรทำ - แสดงความคิดเห็นอย่างจริงใจ ตรงไปตรงมา เช่น เป็นกำลังใจให้นะ มีอะไรให้ช่วยบอกนะ สู้ ๆ นะ ส่งสติเกอร์ช่วยโย

- ตระหนักอยู่เสมอว่า ไม่เพียงแค่ว่าเราเป็นผู้สื่อสารกับคนนั้นเท่านั้น แต่ยังมีอีกหลายคนเป็นเพื่อนเขา ระวังระวังก่อนที่จะแสดงความคิดเห็นอะไรลงไปเพราะอาจเป็นดราม่าได้

ไม่ควรทำ - แสดงความเห็นหยอกล้อ ให้ความรู้สึกสนุกสนานในโลกดิจิทัลแตกต่างออกไป การโพสต์แสดงความคิดเห็นอาจจะไปจี้ปมในใจเนื่องจาก อาจจะตีความหมายในการสื่อสารผิดได้ (ตัวหนังสือไม่มีน้ำเสียงและความรู้สึก)

กรณีที่ ๒ เห็นเพื่อนของเพื่อนกดโธร ภายใต้ภาพงานแต่งของเรา

ควรทำ - นั่งเฉยไป เข้าใจว่าเป็นการกดผิด หากคิดถึงตัวเอง เราอาจจะกดภาพแสดงความรู้สึกในโพสต์ผิดได้ ดังนั้นควรมีวิจารณญาณในการตีความ

ไม่ควรทำ - ไม่ควรไว้วางใจ ต่อว่าคำนิททั้งต่อหน้าและในโพสต์ หรือคอมเมนต์ หรือไปนินทาลับหลัง

กรณีที่ ๓ เมื่อเราเห็นเพื่อนสนิทของเราโพสต์ข้อความว่า ตกงาน ไม่มีงานทำ อยู่ในสภาวะเศรษฐกิจตกต่ำ ควรทำ - โพสต์หรือคอมเมนต์ให้กำลังใจพร้อมสนับสนุน ให้คำแนะนำในช่องทางตัว ยิงในโลกดิจิทัล เป็นพื้นที่สาธารณะเราควรระวังการตอบโต้ หรือแสดงความคิดเห็น

ไม่ควรทำ - คอมเมนต์สั่งสอน สื่อในเชิงลดทอนกำลังใจ หรือซ้ำเติม เชิงลบ

ข้อระวังเนื้อหาในการโพสต์

- ๑) เนื้อหา หรือรูปภาพ ที่เป็นลิขสิทธิ์ของผู้อื่น
- ๒) เนื้อหา หรือรูปภาพอาจทำให้เกิดความขัดแย้งด้านความเชื่อ และศาสนา
- ๓) เนื้อหา หรือรูปภาพ แสดงความรุนแรงและทารุณ
- ๔) เนื้อหา หรือรูปภาพแอบถ่าย หรือภาพบุคคลอื่นที่ไม่ได้รับอนุญาต

การใช้เทคโนโลยีตอบโต้ แสดงความเห็น หรือมีปฏิสัมพันธ์ในการติดตามเนื้อหาในด้านดิจิทัล มีผลกระทบต่อสุขภาพจิตของตัวเองและผู้อื่น ดังนั้นเราควรใช้ข้อความสื่อสารในเชิงบวก ไม่ทำให้ผู้อื่นเกิดความเสียหาย หรือกระทบจิตใจ เมื่อโพสต์ คอมเมนต์ เผยแพร่ สื่อ เนื้อหาใด ๆ ควรคิดไตร่ตรองอย่างน้อย ๓ ครั้ง โปรดตั้งคำถามเสมอในการสื่อสาร เนื้อหาในการเผยแพร่ว่า เมื่อผู้อื่นเห็น หรือได้อ่าน ผู้อื่นจะรู้สึกอย่างไร

๓. การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security)

๓.๑ การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security)

๑) การล่วงละเมิดทางไซเบอร์ (Cyber Abuse) คือการแสดงพฤติกรรมที่เป็นอันตราย สร้างความรำคาญ หรือสร้างความเสียหายให้กับผู้อื่น ทั้งความรู้สึก ทรัพย์สิน หรือการละเมิดในชีวิตจริง บนเครือข่ายออนไลน์ต่าง ๆ

- การกระหน่ำทางไซเบอร์ (Cyberbullying)
- การรังควานทางไซเบอร์ (Cyber Harassment)
- การสะกดรอยตามทางไซเบอร์ (Cyber Stalking)
- การก่อกวน (Trolling)

สาเหตุของการล่วงละเมิด

- ต้องการก่อกวนโดยไม่มีสาเหตุ หรือเรียกว่านักเลงคีย์บอร์ด
- ต้องการแกล้งกันเล็ก ๆ น้อย ๆ
- แกล้งกันจนขัดแย้งบานปลาย กลายเป็นเรื่องใหญ่ หรือจากความขัดแย้งรุนแรงแต่แรกแล้วใช้พื้นที่ใน

โลกออนไลน์โจมตีอีกฝ่าย

- ต้องการรังควาน ผู้ที่เป็นเป้าหมาย หรือผู้ที่ขัดแย้งกันอยู่
- ต้องการข่มขู่ หรือสร้างความหวาดกลัว ให้กับผู้อื่นที่เป็นเป้าหมาย หรือผู้ที่ขัดแย้งกันอย่างรุนแรง
- ติดตามไปประสังครายในชีวิตจริง

สาเหตุของภัยคุกคามทางไซเบอร์

- การตั้งพาสเวิร์ดที่ง่ายเกินไป มีคนใช้รหัสผ่าน “๑๒๓๔๕๖” นับล้านบัญชี เนื่องจากง่าย และยังใช้รหัสผ่านเดียวกันในหลายเว็บไซต์ เปิดโอกาสให้ผู้ประสังครายเข้าถึงข้อมูลได้

- โปรแกรมรักษาความปลอดภัยไม่ทำงาน อุปกรณ์มีโปรแกรมรักษาความปลอดภัยแต่ในบางครั้งอาจไม่ทำงาน หรือทำงานไม่เต็มที่ เนื่องจากติดลิขสิทธิ์ หรือขาดการอัปเดต

- ความประมาท ผู้ประสังครายในโลกดิจิทัลมักจะจ้องเล่นงานโจมตีช่องโหว่ ผู้ที่ไม่ระมัดระวัง หรือประมาท เกิดจากการกดรับโพสต์ หรือลิงก์จากผู้อื่น

ผลกระทบของภัยคุกคามทางไซเบอร์

- ตัวบุคคล ผู้ประสงค์ร้ายสามารถคุกคาม เพื่อนำข้อมูลส่วนบุคคลไปใช้แอบอ้างเพื่อผลประโยชน์ทางทรัพย์สิน และความสัมพันธ์ได้

- อุปกรณ์และระบบต่าง ๆ ผู้ประสงค์ร้ายสามารถโจมตีให้อุปกรณ์และระบบ ไม่สามารถใช้งานได้เพื่อเรียกเก็บเงินค่าไถ่เพื่อให้ใช้อุปกรณ์ได้ดังเดิม

รูปแบบของการล่วงละเมิดทางไซเบอร์

๑) การรรานทางไซเบอร์ (Cyber bullying) : การกลั่นแกล้ง การให้ร้าย การด่าว่า การข่มเหง หรือการรังแกผู้อื่นในโลกดิจิทัล เช่น โซเชียลมีเดียต่าง ๆ

๒) การรังควาญทางไซเบอร์ (Cyber Harassment) : การล่วงละเมิดทางไซเบอร์ที่ร้ายแรงกว่า พัฒนาจากการรรานทางไซเบอร์ โดยการส่งข้อความ หรือคอมเมนต์ทำร้ายจิตใจ ทำให้รู้สึกไม่สบายใจ หรือถูกข่มขู่ ด่าทออย่างต่อเนื่อง พัฒนาไปถึงการสะกดรอยตามทางไซเบอร์

๓) การสะกดรอยตามทางไซเบอร์ (Cyber Stalking) : การติดต่อหรือส่งข้อความมาซ้ำ ๆ อย่างต่อเนื่องจากบุคคลที่เราไม่ต้องการ เกิดจากแรงจูงใจต่าง ๆ มากมาย เช่น อารมณ์ ความรู้สึก อาจพัฒนามาจากการรังควาญบ่อยครั้งลุกลามไปยังการล่วงละเมิดต่าง ๆ ในโลกความเป็นจริง

๔) การเกเรียน (Trolling) : คือการจงใจโพสต์ หรือคอมเมนต์ข้อความที่ยั่วแหย่ ทำให้เสียอารมณ์ ตกใจ ทะเลาะกับคนอื่น การเกเรียนมีหลายรูปแบบ แต่มักเป็นประเด็นขัดแย้ง

คำแนะนำในการท่องโลกดิจิทัล

๑) ตรวจสอบก่อนรับเป็นเพื่อน โดยรับเฉพาะคนที่รู้จักในชีวิตจริง

๒) บล็อกคนที่เคยติดต่อด้วย ข้อความในแง่ลบ หรือไม่ปลอดภัย

๓) คิดให้รอบคอบ เกี่ยวกับการแชร์ลิงก์ไปยังเว็บไซต์ หรือโซเชียลมีเดียต่าง ๆ บางครั้งอาจเจอลักษณะลิงก์ย่อ ควรตรวจสอบข้อมูลดี ๆ

๔) คิดก่อนอัปโหลดและแชร์รูปภาพ ควรคิด และระวังก่อนโพสต์รูป ทั้งรูปส่วนตัวและรูปครอบครัว

๕) คำนิ่งถึงสิ่งที่เขียนถึงผู้อื่น เราไม่มีทางรู้ว่าใครจะอ่านความคิดเห็นเหล่านี้ และพวกเขาจะตีความอย่างไร

๖) ให้เพื่อนออนไลน์อยู่แค่บนโลกออนไลน์เท่านั้น อย่าตกลงที่จะพบคนที่รู้จักบนโลกออนไลน์เพียงลำพัง พาเพื่อนหรือครอบครัวไปด้วย

๗) ระวังเรื่องเพศสัมพันธ์ทางออนไลน์ ระวังการส่งหรือได้รับข้อความบรรยายในเรื่องเซ็กส์อย่างโจ่งครึ่ม

๘) ป้องกันตัวตนของเรา เลือกชื่อผู้ใช้ที่ไม่ใช่ของจริง และรูปโปรไฟล์ที่ไม่แสดงข้อมูลส่วนบุคคลใด ๆ

๙) นึกถึงความเป็นส่วนตัว หลีกเลี่ยงการแบ่งปันข้อมูลส่วนบุคคลทางออนไลน์ที่อาจนำไปใช้ในทางที่ผิดโดยบุคคลอื่นในชีวิตจริง

ภัยคุกคามทางไซเบอร์ (Cyber Threat) มีรูปแบบดังนี้

๑) อีเมลอันตราย อีเมลที่เหมือนมาจากระบบ หรืออื่น ๆ หากกดรับบัญชีจะถูกบุกรุก เพื่อให้ได้ข้อมูลส่วนบุคคล หรือเสียหาย เช่น กิจกรรมแจกรางวัล ธนาคาร หรือแอบกระเป่าเงินต่าง ๆ เว็บไซต์ขายของออนไลน์ หน่วยงานรัฐ หรือธุรกิจอื่น ๆ ควรตรวจสอบอีเมลให้ดีกว่า

๒) สเปน (Spam) อีเมลที่มีข้อความที่ส่งให้ผู้รับโดยไม่ได้รับอนุญาต และไม่เปิดโอกาสให้ปฏิเสธข้อความ ซึ่งก่อให้เกิดความรำคาญ อีเมลไม่ระบุว่าเป็นใคร

๓) ฟิชซิง (Phishing) การหลอกลวงให้เหยื่อคลิก หรือให้เหยื่อกรอกข้อมูลส่วนตัว คำว่าฟิชซิง คล้าย การตกปลาเพื่อล่อเหยื่อ

๔) มัลแวร์ (Malware) โปรแกรมที่สร้างความเสียหายต่ออุปกรณ์ไอที ตั้งแต่การเข้าควบคุมระบบ คอมพิวเตอร์ โทรศัพท์มือถือ เปลี่ยนรหัสผ่าน แก้ไขข้อมูลต่าง ๆ หรือส่งข้อความรบกวน รวมถึงเรียกค่าไถ่

๕) ภัยที่มาจากการชอปปิงออนไลน์ รูปแบบนี้ทำให้นักต้มตุ๋นมีช่องทางมากขึ้นในการหลอกให้เรา จ่ายเงิน

๖) ภัยจากการไม่สำรองข้อมูล การจัดเก็บข้อมูลทั้งหมดไว้บนคอมพิวเตอร์ มีความเสี่ยงที่จะสูญหายได้

เว็บไซต์ที่แนะนำในการตรวจสอบ หรือติดตามสถานการณ์การคุกคามทางโลกดิจิทัล เว็บไซต์แรกคือ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) และศูนย์ปราบปรามอาชญากรรม ถ้าพบเจอปัญหาต่าง ๆ เรา สามารถแจ้งความออนไลน์ โดยเฉพาะคดีทางเทคโนโลยีเราสามารถทำตามขั้นตอนได้

๔. การรู้เท่าทันดิจิทัล (Digital Literacy)

๔.๑ การใช้งานสื่อสารสนเทศ (Media and Information Use)

แหล่งข้อมูลดิจิทัล คือแหล่งข้อมูลที่ถูกสร้างขึ้น หรือแปลงสภาพมาจากอนาล็อก ให้มาเป็นในรูปแบบของ ดิจิทัล ซึ่งสามารถค้นหา เข้าถึง นำเข้าข้อมูล ในการผ่านระบบอินเทอร์เน็ต เช่น เว็บไซต์ที่ทำให้ดูข้อมูลสุขภาพ ข่าวสาร บทความ รวมทั้งเว็บไซต์ที่รวบรวมข้อมูลภาพ เพลง หรือรายการบันเทิง ดังนั้นเราสามารถเข้าชมผ่าน คอมพิวเตอร์ โทรศัพท์มือถือ โดยใช้อินเทอร์เน็ต

รูปแบบของแหล่งข้อมูลดิจิทัล

๑) แบ่งตามแหล่งที่เผยแพร่ข้อมูล

- การสร้างหรือผลิตข้อมูลโดยเจ้าของแหล่งข้อมูล เช่น ข้อมูลจากเว็บไซต์โรงพยาบาล หน่วยงานรัฐ หรือเอกชนต่าง ๆ

- การสร้าง หรือผลิตข้อมูลโดยชุมชนผู้ใช้งาน เช่น เฟซบุ๊ก ทวิตทีย์ และโซเชียลมีเดีย เป็นต้น

๒) แบ่งตามสิทธิ์การเข้าถึงข้อมูล

- แหล่งข้อมูลที่สามารถเข้าถึงได้โดยเสรี ไม่มีการจำกัดการเข้าถึงข้อมูล เช่นเว็บไซต์ที่เผยแพร่ข้อมูล

- แหล่งข้อมูลที่จำกัดการเข้าถึง ซึ่งสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตที่มีส่วนเกี่ยวข้อง เช่น ระบบทะเบียนราษฎร์ ฐานข้อมูลภาครัฐ

๓) แบ่งตามประเภทของข้อมูล

- แหล่งข้อมูลเพื่อการศึกษาเรียนรู้

- แหล่งข้อมูลเพื่อความบันเทิง

- แหล่งข้อมูลด้านสุขภาพ

- แหล่งข้อมูลด้านธุรกรรม

- แหล่งข้อมูลด้านเศรษฐศาสตร์และธุรกิจ

เกณฑ์ประเมินคุณภาพของข้อมูลจากสื่อดิจิทัล และลักษณะข้อมูลที่มีคุณภาพ

๑) ทันสมัยอยู่ หรือไม่

- ข้อมูลเป็นปัจจุบัน หรือมีการอัปเดต

- วันที่เผยแพร่ข้อมูล หากนานแล้วต้องพิจารณา

- ลิงก์เว็บยังสามารถเปิดได้

- แผนภูมิและกราฟ มีวันที่รวบรวม

๒) ตอบโจทย์การใช้งานของเราหรือไม่

- มีเนื้อหาเกี่ยวข้องกับเรื่องที่เราต้องการ
- วัตถุประสงค์ของเนื้อหาตรงตามความต้องการ
- นำเสนอเนื้อหาสำหรับกลุ่มเป้าหมายที่ตรงกับตัวเรา

๓) นำเสนอข้อเท็จจริง หรือเป็นความคิดเห็น มีอคติ หรือแหล่งอ้างอิงหรือไม่

- เนื้อหาใช้ภาษาถูกต้องตามหลักไวยากรณ์
- ข้อมูลถูกต้อง และสามารถตรวจสอบได้
- มีอ้างอิงแหล่งที่มาของข้อมูล
- การนำเสนอข้อมูลดูมีความเป็นมืออาชีพ มีสถิติ หรือผลการตรวจสอบรองรับ

๔) ผู้เขียน หรือผู้นำเสนอข้อมูล มีความเชี่ยวชาญในเรื่องนั้นหรือไม่

- มีการระบุผู้เขียนชัดเจน
- มีรายละเอียดเกี่ยวกับผู้เขียนชัดเจน
- ผู้เขียนมีความเชี่ยวชาญ ประสบการณ์ คุณวุฒิเหมาะสมกับเนื้อหา มีข้อมูลในการติดต่อผู้เขียน

๕) วัตถุประสงค์ที่แท้จริงของข้อมูลนี้คืออะไร เพื่อแจ้งให้ทราบ หรือชวนเชื่อหรือไม่

- เผยแพร่ข้อมูลโดยองค์กรที่มีชื่อเสียงและน่าเชื่อถือ

การประเมินความน่าเชื่อถือ ของข้อมูลในโลกดิจิทัล

๑) ตรวจสอบผู้เขียน มีการระบุผู้เขียนชัดเจน มีรายละเอียดเกี่ยวกับผู้เขียนชัดเจน ผู้เขียนมีชื่อเสียง หรือเชี่ยวชาญในเรื่องนั้น

๒) ตรวจสอบเนื้อหา เนื้อหาอ่านเข้าใจง่าย ใช้ภาษาที่ถูกต้อง เนื้อหามีความถูกต้อง เทียงตรง แม่นยำ มีสถิติ มีการอ้างอิงแหล่งที่มา

๓) ตรวจสอบผู้เผยแพร่ หรือแหล่งข้อมูล เผยแพร่ในแหล่งที่มีชื่อเสียง น่าเชื่อถือ มีเนื้อหาตรง วัตถุประสงค์ในการรวบรวมแหล่งข้อมูลนั้น ผู้เผยแพร่ไม่ได้มีส่วนได้ส่วนเสีย

๔) ตรวจสอบเวลาที่เผยแพร่ ข้อมูลมีความทันสมัย แสดงวันที่ในการอัปเดตข้อมูลชัดเจน ลิงก์ข้อมูลยังสามารถใช้งานได้ เนื้อหาข้างในสมบูรณ์

การสืบค้นข้อมูลจากสื่อดิจิทัล

๑) คำค้น หรือคีย์เวิร์ด - กำหนดคำ หรือประโยคคำค้น

๒) เครื่องมือค้นหา - การเลือกข้อมูลที่เหมาะสม

๓) เทคนิคในการช่วยค้น เช่น ใช้ Advanced Search ในการช่วยค้นหาบน Google หรือใช้โปรแกรมคอมพิวเตอร์ หรือโทรศัพท์มือถือได้

ลักษณะของข้อมูลที่มีคุณภาพ

๑) ข้อมูลประเภทตัวอักษร (Text, text) เช่น Google Search เว็บไซต์หอสมุดโรงเรียน หรือมหาวิทยาลัยต่าง ๆ

๒) ข้อมูลประเภทรูปภาพ เช่น Pinterest, Google Image, Pixabay

๓) ข้อมูลประเภทวิดีโอ เช่น YouTube, Vimeo, Pixabay , Google

๔) ข้อมูลประเภทเสียง เช่น YouTube Audio Library

เครื่องมือที่ใช้ในการรวบรวมข้อมูล

๑) สำหรับการรวบรวมข้อมูล ประเภทข้อมูล

- Google Drive พื้นที่เก็บข้อมูลที่มีความปลอดภัย
- iCloud บริการเชื่อมต่อกับอุปกรณ์ Apple
- Dropbox เครื่องมือฝากเอกสารออนไลน์
- One Drive ระบบคลาวด์ของ Microsoft

๒) สำหรับการรวบรวมข้อมูลที่เป็นไอเดีย เน้นการติดต่อสื่อสาร

- Line สามารถสร้างแชต หรือสร้างกลุ่ม และโพสต์รูปต่าง ๆ
- Facebook เหมาะสำหรับการสนทนาในวงจำกัด สื่อสารแบบกลุ่ม
- OneNote สมุดบันทึกดิจิทัล เก็บได้ทั้งอักษรและรูปภาพ
- Google Keep ช่วยเก็บหรือบันทึกข้อมูล เก็บไว้บนออนไลน์

ผลจากการแบ่งปันเนื้อหาที่ไม่เหมาะสม

การกระทำ/พฤติกรรม

ผลกระทบทางกฎหมาย

ผลกระทบทางจริยธรรม

- | | | |
|---|--|--|
| - ฝากร้านขายของ และส่งข้อความ
ก่อกวนโดยไม่ได้รับอนุญาต | - มีความผิดปรับไม่เกิน ๒ แสนบาท | - ทำให้ผู้อื่นเกิดความรำคาญ |
| - โพสต์หรือแชร์ข้อมูลเท็จ ที่สร้าง
ความเสียหายต่อบุคคลหรือประเทศ | - จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน
๑ แสนบาท และระงับข้อมูล | - เกิดความเข้าใจผิดและอับอาย สร้าง
ความเกลียดชัง ทำให้เสียชื่อเสียง |
| - โพสต์ข้อมูลปลอม ข้อมูลทุจริต
หลอกลวงที่สร้างความเสียหายต่อ
ความมั่นคง | - จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑
แสนบาท และระงับข้อมูลนั้น หรือ
ลงโทษตามมาตรา | - เกิดความตื่นตระหนก การขัดแย้ง
ทางสังคม การตัดสินใจผิดพลาดได้ |
| - โพสต์ หรือแชร์ข้อมูล ภาพตัดต่อ
ที่สร้างความเสียหายต่อผู้อื่น | - จำคุกไม่เกิน ๓ ปี ปรับไม่เกิน
๒ แสนบาท และระงับข้อมูลนั้น | - สร้างความอึดอัดใจ ความสะเทือนใจ
และความรู้สึกหดหู่ใจ |

๔.๒ ผู้จัดทำสื่อและสารสนเทศ (Media and Information Creative)

ประเภทเนื้อหาดิจิทัล

๑) เนื้อหาดิจิทัลเกี่ยวกับสุขภาพอนามัย : เกี่ยวกับการดูแลสุขภาพ สาเหตุการเกิดโรคต่าง ๆ วิธีการป้องกันการเกิดโรคร้าย จัดทำขึ้นโดยหน่วยงานทางสุขภาพ

๒) เนื้อหาดิจิทัลเกี่ยวกับข้อมูลภาครัฐ : การให้บริการข้อมูลต่าง ๆ ของภาครัฐ สิทธิ และหน้าที่ของประชาชนในเรื่องต่าง ๆ กฎหมาย ระเบียบ คำสั่ง แนวปฏิบัติ เป็นต้น ซึ่งออกโดยภาครัฐ ทั้งนี้เนื้อหาของข้อมูลภาครัฐจะสร้างขึ้นหรือเผยแพร่ในหน่วยงานของภาครัฐ อาจเป็นกระทรวง กรม หรือกองต่าง ๆ

๓) เนื้อหาดิจิทัลเพื่อความบันเทิง : ตอบสนองความต้องการความบันเทิง เช่น ภาพยนตร์ นิยาย รายการเพลง จัดทำขึ้นโดยบริษัท หรือผู้ประกอบการด้านบันเทิง

๔) เนื้อหาดิจิทัลด้านการตลาด : เพื่อซื้อขายหรือสร้างแรงจูงใจให้เกิดการซื้อขายหรือบริการ ผลิตโดยบริษัท หรือห้างร้านที่ทำธุรกิจ หรือบุคคลทั่วไปอาจเป็นพนักงาน หรือผู้ประกอบการ

๕) เนื้อหาดิจิทัลที่ใช้สำหรับการศึกษาและเรียนรู้ : ทั้งการศึกษาที่อยู่ในระบบ และการศึกษาเรียนรู้ตามอัธยาศัย จัดทำขึ้นโดยสถาบันการศึกษา หรือผู้เชี่ยวชาญ บุคลากรทางวิชาการ หรือผลิตโดยผู้ชำนาญ

๖) เนื้อหาดิจิทัลด้านข่าวสาร : รายงานความเคลื่อนไหวที่เกิดขึ้นในสังคม อาจเป็นด้านธุรกิจ ด้านการศึกษา หรือเหตุการณ์ทั่วไป

ประเภทของสื่อดิจิทัล

๑) รูปภาพดิจิทัล สร้างขึ้นเพื่อบันทึกเรื่องราว เหตุการณ์ของ คน สัตว์ สิ่งของ ที่นิ่งอยู่กับที่ อาจเป็นภาพถ่าย หรือภาพสแกน ภาพวาดที่สร้างขึ้นด้วยโปรแกรมคอมพิวเตอร์ โดยรูปดิจิทัลสามารถสร้างขึ้นด้วยกล้องถ่ายรูปของโทรศัพท์มือถือ ภาพถ่ายหน้าจอโทรศัพท์ หรือการสแกนสิ่งพิมพ์แล้วนำเข้าเครื่องคอมพิวเตอร์

๒) ข้อความดิจิทัล เป็นข้อความที่สร้างขึ้นเพื่อบอกเล่าเหตุการณ์ สื่อสารให้ความรู้ หรือสร้างความเข้าใจให้ตรงกัน ในรูปแบบของการพิมพ์ ผลิตโดยโปรแกรมคอมพิวเตอร์ หรือผ่านแอปพลิเคชันในโทรศัพท์มือถือ

๓) เสียง เป็นสื่อที่สร้างขึ้นสำหรับการบรรยายโดยใช้อุปกรณ์บันทึกเสียง หรือโปรแกรมคอมพิวเตอร์ เล่าเหตุการณ์ ความรู้สึก เพลง เรื่องราว ดนตรี หรือเสียงอย่างอื่น สามารถสร้างขึ้นได้โดยบันทึกด้วยอุปกรณ์บันทึกเสียง หรืออาจจะใช้โทรศัพท์ในการบันทึก หรือสร้างขึ้นจากโปรแกรมคอมพิวเตอร์

๔) วิดีโอ เป็นการผสมของเสียงและภาพ สร้างด้วยโทรศัพท์ หรือกล้องวิดีโอ โดยนำภาพนิ่งหลาย ๆ ภาพในเวลาสั้น ๆ จนกลายเป็นภาพเคลื่อนไหว และนำไปผสมกับเสียง

๕) ภาพกราฟิกดิจิทัล สร้างขึ้นแทนการสื่อความหมาย เพื่อให้เกิดความเข้าใจในข้อมูลที่ซับซ้อน เช่น กราฟ แผนภูมิ อินโฟกราฟิก เป็นต้น

หลักการสร้างเนื้อหา ให้ถูกกฎหมายและมีจริยธรรม

ลิขสิทธิ์ กับ Creative Commons

๑) ลิขสิทธิ์แบบเดิม ห้ามทุกคนทำทุกอย่าง เป็นกรอบแนวคิดของสมัยเดิมก่อนเกิดเทคโนโลยีสารสนเทศ และแลกเปลี่ยนข้อมูลผ่านอินเทอร์เน็ต

๒) Creative Commons เสนอทางเลือกที่เจ้าของลิขสิทธิ์ สามารถแบ่งปันข้อมูลได้ เลือกสงวนสิทธิ์ตามที่ต้องการได้ ตรงใจ ตรงไลฟ์สไตล์

ประเภทและรูปแบบของ Creative Commons (CC license)

เราสามารถเลือกทางเลือก ในการลิขสิทธิ์ ในการแบ่งปันข้อมูล สงวนลิขสิทธิ์ไม่แบ่งปันได้ เพื่อช่วยให้โลกเข้าถึงผลงานในการสร้างสรรค์ได้มากขึ้น โดยเสนอแบบสัญญาอนุญาต CC license ให้เลือก ๖ แบบ โดยเจ้าของลิขสิทธิ์เพียงเลือกสัญญาตามไอคอน ๔ ชนิด ดังนี้ ๑) Attribution (BY) ๒) Share Alike (SA) ๓) Non-Commercial (NC) ๔) No Derivative Works (ND)

๑) Attribution : CCBY สามารถแจกจ่าย เปลี่ยนแปลง ดัดแปลง ใช้งานอย่างไรก็ได้ รวมถึงการค้า และต้องมีอ้างอิง

๒) Attribution Share Alike : CCBY - SA ยอมให้เปลี่ยนแปลง ดัดแปลง รวมถึงการค้า และต้องมีอ้างอิง

๓) Attribution No Derivative Works : CCBY - ND ยอมให้ใช้ และแจกจ่ายต่อ รวมถึงการค้า และต้องมีอ้างอิง แต่ห้ามดัดแปลง

๔) Attribution Non-Commercial : CCBY - NC ยอมให้เปลี่ยนแปลง ดัดแปลง และต้องมีอ้างอิง แต่ห้ามใช้ทางการค้า

๕) Attribution - Non-Commercial - No Derivative Works : CCBY - NC - ND แบ่งปันน้อยที่สุดใน ๖ แบบ ห้ามดัดแปลง ห้ามใช้ทางการค้า แต่ต้องมีอ้างอิง

๖) Attribution - Non-Commercial - Share Alike : CCBY - NC - SA อนุญาตเผยแพร่ ดัดแปลง แต่ห้ามใช้ทางการค้า และต้องมีอ้างอิง

วิธีการเช็กสิทธิ์สื่อ ก่อนนำมาใช้

ใช้ได้ ได้แก่ การสร้างรูปภาพนั้นขึ้นมาเอง ใช้ภาพของผู้อื่นเพื่อรายงานการศึกษา งานวิจัย และการใช้ภาพของผู้อื่นที่มี Creative Commons เพื่อการค้าหรือกำไรส่วนบุคคล โดยใช้งานตามเงื่อนไขที่อนุญาต

ใช้ไม่ได้เลย ได้แก่ ภาพของผู้อื่นที่ไม่ได้รับอนุญาตจากแหล่งต้นฉบับ การใช้ภาพของผู้อื่นเพื่อการค้า หรือกำไรส่วนบุคคล โดยไม่จ่ายเงินเพื่อใช้รูปภาพ

ผลจากการสร้างเนื้อหาที่ละเมิดกฎหมาย และจริยธรรม

พฤติกรรมการสร้างเนื้อหาที่ละเมิดกฎหมาย

กฎหมายที่ละเมิด พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี๒๕๕๐ และ ๒๕๖๐

- การให้ข้อมูลเกี่ยวกับการเสียชีวิตต้องไม่ทำให้เกิด
ความเสื่อมเสียชื่อเสียง

- มาตรา ๑๖ ระวังโทษจำคุกไม่เกิน ๓ ปี ปรับไม่เกิน
๒ แสนบาท

- การโพสต์ด่าว่าผู้อื่น มีกฎหมายอาญาอยู่แล้ว ไม่มี
ความจริง หรือถูกตัดต่อ ผู้กล่าวหาสามารถเอาผิดได้

- ม. ๑๔ (๑) (๕) ระวังโทษจำคุกไม่เกิน ๓-๕ ปี ปรับ
ไม่เกิน ๖ หมื่นบาท ถึง ๑ แสนบาท หรือทั้งจำทั้งปรับ

- ทำการละเมิดลิขสิทธิ์ผู้ใด ไม่ว่าจะข้อความ เพลง
เกิน

- ม.๑๔ (๕) ระวังโทษจำคุก ไม่เกิน ๕ ปี หรือปรับไม่
เกิน

รูปภาพ หรือวิดีโอ

๑ แสนบาท หรือทั้งจำทั้งปรับ

- ส่งรูปภาพแชร์ของผู้อื่น เช่น สิวสตีวันจันทร์
ถือว่าไม่ผิด ถ้าไม่นำไปหารายได้

- ไม่มีความผิด

๕. การสื่อสารดิจิทัล (Digital communication)

๕.๑ ร่องรอยดิจิทัล (Digital Foot print)

หากเปรียบเทียบกับกระทำความผิดในโลกความเป็นจริง ก็เหมือนกับการที่เราไปสถานที่ต่าง ๆ เมื่อเราเดินผ่านก็จะเกิดรอยเท้า หรือการขีดเขียนผนังก็จะเกิดร่องรอยขีดเขียนทิ้งไว้ เมื่อเดินผ่านใครสักคนก็อาจจะจดจำเราได้ เมื่อต้องการให้มีการติดตามตัวเรา ก็จะต้องอาศัยร่องรอยเหล่านี้ ในการติดตามตัวเราในโลกดิจิทัล

ร่องรอยดิจิทัล คือข้อมูลพฤติกรรมในการใช้งานในโลกดิจิทัลของเรา ซึ่งระบบจะบันทึกไว้ทั้งหมด ร่องรอยดิจิทัลเกิดขึ้นจากการใช้งานโลกของดิจิทัลไม่ว่าจะเป็นการค้นหาข้อมูล ค้นหาสินค้าและบริการ การใช้งานโซเชียลมีเดียต่าง ๆ ทั้งโพสต์ คอมเมนต์ และการแชร์เนื้อหาต่าง ๆ หรือแม้กระทั่งการพูดคุยส่วนตัว แม้ว่าเราจะคิดว่าเป็นความลับ แต่ก็เป็นการสร้างร่องรอยดิจิทัล

ร่องรอยดิจิทัลเชิงบวก

- โพสต์อย่างสร้างสรรค์ เป็นกลาง ชื่นชม ด้วยความเข้าใจ หากต้องการกล่าวถึงผู้อื่นในโลกดิจิทัล พยายามใช้เพียงข้อเท็จจริง และระวังข้อความ หรือรูปที่ทำให้คนอื่นเสียหายได้

- แสดงความคิดเห็นในโพสต์ หรือแชตด้วยข้อความที่สุภาพ ไม่ด่าทอ หรือดูถูกความคิดของผู้อื่น แม้อาจจะเห็นต่าง ผลคือทำให้เรามีมารยาทที่ดี สังคมสร้างสรรค์

- ค้นหาข้อมูลที่เป็นประโยชน์ และสร้างสรรค์ เช่น การหาข้อมูลสุขภาพอยู่เป็นประจำ ระบบจะเก็บประวัติการค้นหา และนำเสนอสิ่งที่เกี่ยวข้องกับคำค้น

ร่องรอยเชิงลบ

- โพสต์พาดพิงถึงผู้อื่นในทางที่ไม่ดี เสียดยศ หรือไม่ระวัง จนทำให้เกิดความเสียหาย หรืออับอาย ในโลกดิจิทัลนั้นเกิดความเข้าใจผิดกันได้ง่าย และยังส่งผลเชิงลบทั้งผู้โพสต์ และผู้ถูกกล่าวถึงได้เช่นกัน

- แสดงความคิดเห็นในโพสต์ของผู้อื่นด้วยข้อความไม่สุภาพ สร้างความขัดแย้ง ซึ่งอาจทำให้เกิดการตอบโต้หรือโต้เถียงกัน โดยอาจส่งผลต่อภาพลักษณ์ดิจิทัลเชิงลบกับเรา

- ค้นหาข้อมูลที่ไม่เป็นประโยชน์ หรือไม่สร้างสรรค์ เช่น การค้นหาข้อมูลเกี่ยวกับความรุนแรง เรื่องเพศ ข้อมูลการพนัน ซึ่งเมื่อค้นหาบ่อย ๆ ระบบจะจดจำ และนำเสนอข้อมูลแบบเดียวกัน

เครื่องมือช่วยจัดการรอยเท้าดิจิทัล

๑) แอปจัดการรหัสผ่าน ดูแลการซิงค์รหัสผ่านกับบัญชีต่าง ๆ และแจ้งเตือนเมื่อรหัสผ่านรั่วไหล รหัสผ่านถือเป็นด่านแรกที่สำคัญมาก ที่ทำให้เกิดร่องรอยดิจิทัล เราจะปลอดภัยหรือถูกรูกล้ำ โดนขโมย แอบอ้าง หรือปลอมแปลงให้เกิดข้อมูลเชิงลบ แอปจัดการรหัสผ่านจะเข้ามาช่วยรวบรวมบัญชีรหัสผ่านต่าง ๆ ของเราได้ ได้แก่ Dropbox Password, ๑Password, Last pass, iCloud Password, Microsoft Authenticator, Chrome Password Manager

๒) แอปหรือเว็บไซต์ช่วยป้องกันการติดตาม จะช่วยป้องกันการติดตามและบันทึกการใช้แอปต่าง ๆ ป้องกันไม่ให้ข้อมูลรั่วไหล เช่น Disconnect, Ghostery, DuckDuckGo, Tor

๓) เครื่องมือค้นหาแบบส่วนตัว เครื่องมือเหล่านี้จะช่วยให้เราค้นหาสิ่งที่ต้องการแบบไม่เปิดเผยตัวตนได้ เช่น Start page, Disconnect Search, DuckDuckGo, Qwant

วิธีการรับมือกับความเสียหายจากรอยเท้าดิจิทัล

๑) ถูกทำให้เสียชื่อเสียงจากโพสต์หรือคอมเมนต์

- ลบ หรือแก้ไขโพสต์ และคอมเมนต์ที่เป็นปัญหา
- ขอโทษผู้อื่นที่ได้รับผลกระทบอย่างจริงจัง
- สร้างร่องรอยใหม่ที่เหมาะสม

๒) ถูกละเมิดข้อมูลส่วนตัว โดยถูกสวมรอยบัญชีต่าง ๆ เช่น เฟซบุ๊ก ไลน์ หรือแอปอื่นๆ ไม่ว่าเราจะถูกสวมรอย หรือคนอื่นถูกสวมรอยก็ตาม ต้องรีบดำเนินการแก้ไขทันที

- กดรีพอร์ต และเปลี่ยนพาสเวิร์ด
- แจ้งเจ้าหน้าที่โทรหา และช่วยกดรีพอร์ต

๓) สูญเสียทรัพย์สินจากการถูกขโมยข้อมูล

- รวบรวมหลักฐานต่าง ๆ เช่น Cap หน้าจอไฟล์ของคนที่มาหลอกลวงเราไว้
- แจ้งความ และลงบันทึกประจำวันกับตำรวจในท้องที่
- โทรสายด่วน OCC ๑๒๑๒ เพื่อแจ้งความร้องเรียน

๔) ถูกตามจากโลเคชันที่แชร์ หรือรูปที่ถูกแท็ก เพื่อป้องกันการถูกติดตามตัวควรปฏิบัติดังนี้

- เช็กอินได้ถ้าไม่ใช่สถานที่ส่วนตัว
- ปิดทางแสดงดลเคชัน
- ตั้งค่าการมองเห็นแค่เฉพาะเพื่อน

๕.๒ การมีปฏิสัมพันธ์ และการสร้างความร่วมมือ (Interaction and Collaboration)

การใช้งานเทคโนโลยีดิจิทัล เพื่อการสื่อสาร และสร้างความร่วมมือ

๑) การสื่อสารระหว่างบุคคล ใช้เทคโนโลยีดิจิทัลสื่อสาร เช่น โทรศัพท์ พิมพ์ข้อความ คอล หรือวิดีโอคอลในห้องสนทนาส่วนตัวผ่านโซเชียลมีเดีย

๒) การสื่อสารระหว่างกลุ่มคน เฉพาะกลุ่มแบบไม่เป็นสาธารณะ ใช้ตั้งกลุ่มเพื่อการสื่อสาร เช่น กลุ่มเฟซบุ๊ก ที่เป็นกลุ่มปิด หรือกลุ่มสนทนาในโซเชียลมีเดีย

๓) การสื่อสารระหว่างกลุ่มคนแบบเป็นสาธารณะ การใช้โพสต์แบบเป็นสาธารณะ เช่น โพสต์บนเฟซบุ๊ก ส่วนตัวแล้วเปิดเป็นสาธารณะ ตั้งกลุ่มเฟซบุ๊กแบบสาธารณะ ตั้งกลุ่มในไลน์แบบเปิด ผู้ที่สนใจสามารถเข้าร่วมได้อย่างอิสระ ไม่ต้องรอถูกเชิญ แต่ต้องปฏิบัติตามข้อกำหนดของกลุ่ม

๖. การปรับตัวในยุคดิจิทัล (Digital Disruption)

แนวทางการปรับตัวของบุคลากรในยุคดิจิทัล

- ๑) ด้านทักษะของเราทั้ง soft skill และ hard skill
- ๒) การจัดการข้อมูลต่าง ๆ
- ๓) การกำหนดเป้าหมาย KP มีสติในการดูงาน การทำงานต่าง ๆ ได้

แนวทางการปรับตัวของบุคลากรในสถานที่ทำงานใหม่

- ๑) ปรับตัวให้เข้ากับวัฒนธรรมองค์กรนั้น
- ๒) รู้จักปรับตัวให้เข้ากับผู้ร่วมงาน ไม่ว่าจะเป็นคนในยุคเดียวกัน หรือต่างยุคกัน ช่วงยุคต่าง ๆ จะมีการใช้เทคโนโลยีที่ต่างกัน

๓) เราต้องมีกระบวนการทำงานต่าง ๆ ที่ชัดเจน

แนวทางการปรับตัวในภาวะผู้นำ เราจะต้องมีทักษะที่สำคัญ คือ

๑) ต้องบริหารคนเป็น เราต้องบริหารควบคุมอารมณ์ของเราได้ การมีอีคิวเป็นสิ่งสำคัญ เช่น คนในเจน Z เก่งเทคโนโลยีอยู่แล้ว ช่วงเกิดโรคระบาด หรือช่วงมีฝุ่น PM ๒.๕ มากจนเป็นอันตราย สามารถสั่งให้ Work from home ได้ การสั่งงานผ่าน Google Meet ประชุมออนไลน์ การใช้ระบบอออฟฟิศ เป็นต้น

๒) การบริหารองค์กร เช่น ภาพรวมของประเทศไทยคือ Thailand ๔.๐ สิ่งที่ต้องรับ องค์กรควรมี

- Road Map แผน กลยุทธ์ ยุทธศาสตร์ ที่วางเป็นระยะ ๔ ปี ๒๐ ปี
- การบริหารจัดการข้อมูล ที่มีอยู่เยอะมากมาใช้ให้เกิดประโยชน์อย่างไร จะสร้างระบบอะไรมารองรับจึงจะได้ประโยชน์จากข้อมูล
- เป็นองค์กรที่ทันกระแสนิยม อะไรที่อยู่ตามกระแสนิยมต่าง ๆ ต้องนำมาปรับใช้ ประยุกต์ใช้กับองค์กร เช่น ยุค ๕G ทำประชาสัมพันธ์แบบ VR, e-book, line QR เป็นต้น

- ควรจะสนับสนุนให้บุคลากร หรือองค์กรมีการเรียนรู้ตลอดชีวิต เช่น การเรียนรู้ผ่าน MOOK

๓) การทำงานร่วมกันในสังคม และวัฒนธรรมดิจิทัล

- การเตรียมพร้อมบุคลากรรับ Digital Refinement
- ตัวเราต้องปรับความคิด (Mindset) ก่อน ลองทำดู ลองเรียนรู้ก่อน
- การ Training ต้องเตรียมพร้อมบุคลากรไว้

๒.๒ ประสบการณ์/ประโยชน์ที่ได้รับการประยุกต์ใช้กับหน่วยงาน

ต่อตนเอง

๑. ทำให้มีความรู้ ความเข้าใจเกี่ยวกับความฉลาดทางดิจิทัล ในการใช้ทักษะดิจิทัลต่าง ๆ
๒. ทำให้อยู่ในโลกดิจิทัลได้อย่างชาญฉลาด และปลอดภัย
- ๓) เพื่อให้ผู้เรียนสามารถเข้าใจการทำงาน สร้างความคุ้นเคย และสามารถนำข้อมูลไปใช้ในการทำงานได้อย่างถูกต้อง และปลอดภัย

ต่อหน่วยงาน/การนำมาประยุกต์ใช้กับหน่วยงาน

สามารถนำความรู้ที่ได้รับไปประยุกต์ใช้ในการทำงานด้านเทคโนโลยีดิจิทัล ทั้งในด้านการใช้ข้อมูลของหน่วยงาน การสื่อสาร การทำงานในยุคดิจิทัล เพื่อตอบสนองการทำงานในยุคดิจิทัลของหน่วยงานได้เป็นอย่างดี

๒.๓ ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

ควรมีการอบรมหลักสูตรเกี่ยวกับการใช้เทคโนโลยีดิจิทัล อย่างต่อเนื่อง เพื่อพัฒนาความรู้ ทักษะทางด้านเทคโนโลยีดิจิทัลของหน่วยงานให้กับนักวิชาการ และสามารถนำความรู้ที่ได้ไปประยุกต์ใช้กับงานต่อไป

ลงชื่อ



(นางสาวจิริชยา คงทน)

ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ

ผู้รายงาน

วันที่ ๑๓ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙

(✓) ทราบ

ลงชื่อ



(นายนันทพล หนองหารพิทักษ์)

ตำแหน่ง ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่ ๑๘ เดือน กพ พ.ศ.

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ จิรัชยา คงทน

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Digital Literacy : ความฉลาดทางดิจิทัล

(Digital Intelligence)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 10 กุมภาพันธ์ 2569

ดีใจที่ได้
ได้

A. H.

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ จิรัชยา คงทน

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
ความรู้ความเข้าใจเกี่ยวกับปัญญาประดิษฐ์ (Artificial Intelligence)
สำหรับบุคลากรภาครัฐทุกระดับ

จำนวนชั่วโมงการเรียนรู้ 1:00 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 6 กุมภาพันธ์ 2569

Ah.

ศิริลักษณ์ คงทน
Sirilak

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



1b7ba5d1