



บันทึกข้อความ

กองนโยบายและแผนการใช้ที่ดิน
เลขที่รับ.....๗๘๑
วันที่.....๙ ก.พ. ๖๙
เวลา.....๑๕.๓๘ น.

ส่วนราชการ กลุ่มเศรษฐกิจที่ดินทางการเกษตร กองนโยบายและแผนการใช้ที่ดิน โทร. ๒๒๑๗

ที่ กษ.๐๘๓๗.๐๓/๑๐๓ วันที่ ๙ กุมภาพันธ์ ๒๕๖๙

เรื่อง รายงานสรุปการอบรม สัมมนา และการพัฒนาความรู้ด้านดิจิทัล

เรียน ผู้อำนวยการกลุ่มเศรษฐกิจที่ดินทางการเกษตร

ตามที่กองการเจ้าหน้าที่กำหนดตัวชี้วัดกลางรายบุคคลด้านการพัฒนาบุคลากร รอบการประเมินที่ ๑ (๑ ตุลาคม ๒๕๖๘-๓๑ มีนาคม ๒๕๖๙) ระดับความสำเร็จของการพัฒนาความรู้ โดยมีการพัฒนาความรู้ด้านดิจิทัล ๒ เรื่อง พร้อมสรุปบทเรียน ๑ เรื่อง ส่งให้ผู้บังคับบัญชาทราบ ภายในวันที่ ๑๘ มีนาคม ๒๕๖๙ นั้น

ในการนี้ ข้าพเจ้าได้เข้ารับการพัฒนาคความรู้ครบทั้ง ๒ เรื่อง ได้แก่ ๑) ความฉลาดทางดิจิทัล (Digital Intelligence) และ ๒) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล (Digital Government Act.) พร้อมทั้งสรุปบทเรียนการพัฒนาความรู้ด้านดิจิทัลของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA) จำนวน ๑ เรื่อง ได้แก่ ความฉลาดทางดิจิทัล (Digital Intelligence) เสร็จเรียบร้อยแล้ว (รายละเอียดตามที่แนบ)

จึงเรียนมาเพื่อโปรดนำเรียน ผอ.กนผ. ลงนามในรายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้ และมอบหมายผู้รับผิดชอบดำเนินการต่อไป

วิรัช บุญเลิศ
(นางสาววัลยา บุญเลิศ)
เศรษฐกรชำนาญการพิเศษ

เรียน ผอ.กนผ.

เพื่อโปรดพิจารณา ลงนามในรายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้ และมอบหมายฝ่ายเลขานุการคณะทำงานกลั่นกรองข้อมูลสรุปความรู้ฯ ดำเนินการต่อไป


(นายธนภุต ผลเกลี้ยง)
ผู้อำนวยการกลุ่มเศรษฐกิจที่ดินทางการเกษตร



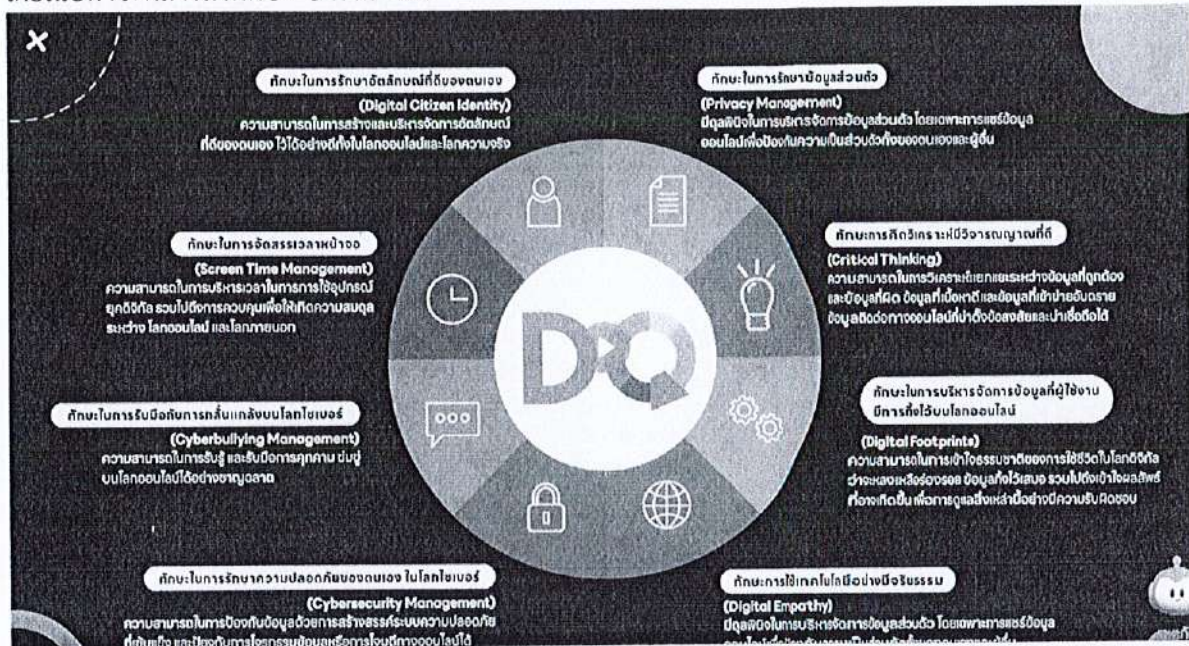
รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

<p>ส่วนที่ 1 ข้อมูลทั่วไป</p> <p>ชื่อ.....นางสาววัลยา.....นามสกุล.....บุญเลิศ..... ตำแหน่ง.....เศรษฐกรชำนาญการพิเศษ.....กลุ่ม/ฝ่าย.....กลุ่มเศรษฐกิจที่ดินทางการเกษตร..... หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ ความฉลาดทางดิจิทัล (Digital Intelligence)..... สถานที่อบรม.....ผ่านระบบ E-Learning ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)..... หน่วยงานที่จัดฝึกอบรม/ประชุม/สัมมนา.....สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)..... ตั้งแต่วันที่ 31 เดือน มกราคม พ.ศ. 2569 ถึงวันที่ 31 เดือน มกราคม พ.ศ. 2569..... เพื่อ <input checked="" type="checkbox"/> อบรม <input type="checkbox"/> สัมมนา <input type="checkbox"/> อื่นๆ ระบุ.....</p>
<p>ส่วนที่ 2 สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้</p> <p>2.1 รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/สัมมนา/พัฒนาความรู้</p> <p>1) คำอธิบายหลักสูตร</p> <p>หลักสูตรเนื้อหาตามมาตรฐาน “ความฉลาดทางดิจิทัล (DQ Digital Intelligence)” จาก DQ Institute ซึ่งเป็นสถาบันที่มีการพัฒนามาตรฐานระดับสากล เกี่ยวกับการให้ความรู้ด้านความฉลาดทางดิจิทัล มาวิเคราะห์ ปรับใช้ให้เหมาะสมกับบริบทของประเทศ</p> <p>2) วัตถุประสงค์หลักสูตร</p> <p>2.1) เพื่อให้ผู้เรียนเข้าใจความหมายและเห็นความสำคัญการสร้างความรู้ความตระหนักรู้ในการใช้อินเทอร์เน็ต</p> <p>2.2) เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับการสร้างความรู้ความตระหนักรู้ในการใช้อินเทอร์เน็ต รู้เท่าทันและมีความมั่นคง ปลอดภัย เพื่อยกระดับวิถีชีวิตด้วยดิจิทัล</p> <p>3) หัวข้อในบทเรียน</p> <p>3.1) Introduction บทนำ</p> <p>(1) ความฉลาดทางดิจิทัล เป็นความสามารถในการใช้เทคโนโลยีดิจิทัล ข้อมูลในการตัดสินใจ และการแก้ปัญหา โดยใช้ความรู้และทักษะทางด้านเทคโนโลยีในการวิเคราะห์ข้อมูลและการประมวลผลข้อมูล</p> <p>(2) ที่มาความฉลาดทางดิจิทัล เป็นผลการศึกษาและพัฒนาตัวเองของ DQ Institute ซึ่งเป็นหน่วยงานที่เกิดจากความร่วมมือของภาครัฐและเอกชนทั่วโลก ร่วมกันประสานงานร่วมกับ World Economic Forum ที่มุ่งมั่นให้เด็ก ๆ ทุกคนในประเทศได้รับการศึกษาทางด้านทักษะพลเมืองดิจิทัลที่มีคุณภาพ และใช้ชีวิตบนโลกออนไลน์อย่างปลอดภัยด้วยความก้าวหน้าของเทคโนโลยีสมัยใหม่</p> <p>(3) ความฉลาดทางดิจิทัลยังเป็นกรอบแนวคิดที่ครอบคลุมความสามารถทางด้านเทคนิคความรู้ ความเข้าใจ และความคิดทางสังคม ที่มีพื้นฐานอยู่ในค่านิยมทางศีลธรรมที่ช่วยให้บุคคลเผชิญหน้ากับความท้าทายทางด้านดิจิทัล</p>

ส่วนที่ 2 (ต่อ)

2.1 รายงานสรุปเนื้อหา (ต่อ)

(3) ความฉลาดทางด้านดิจิทัลมี 3 ระดับ 8 ด้าน ประกอบด้วย ความรู้ ทักษะ ทัศนคติ และค่านิยม โดยเนื้อหาจะกล่าวถึงทักษะ 8 ด้าน ดังนี้



(3.1) ทักษะในการรักษาอัตลักษณ์ที่ดีของตนเอง (Digital Citizen Identity) เป็นการเรียนรู้การพัฒนา การสื่อสารกับผู้อื่น การนับถือตนเองและนับถือผู้อื่น การป้องกันตนเองและป้องกันผู้อื่น

(3.2) ทักษะการคิดวิเคราะห์ที่มีวิจารณญาณที่ดี (Critical Thinking) เป็นการวิเคราะห์แยกแยะระหว่างข้อมูลที่ถูกต้องและข้อมูลที่ผิด ข้อมูลที่เนื้อหาดีและข้อมูลที่เข้าข่ายอันตราย ข้อมูลติดต่อทางออนไลน์ที่น่าเชื่อถือสงสัยและน่าเชื่อถือได้ ซึ่งคือ การประยุกต์ การวิเคราะห์ การสังเคราะห์ และการประเมิน

(3.3) ทักษะในการรักษาความปลอดภัยของตนเองในโลกดิจิทัลไซเบอร์ (Cybersecurity Management) เพื่อรักษาความเป็นส่วนตัวและความลับ ป้องกันการขโมยอัตลักษณ์ ป้องกันการโจรกรรมของข้อมูล และเพื่อป้องกันความเสียหายของข้อมูลและอุปกรณ์

(3.4) ทักษะในการรักษาข้อมูลส่วนตัว (Privacy Management) คือ ไม่ควรตั้งรหัสผ่านของบัญชีที่ง่ายเกินไป ตั้งรหัสผ่านหน้าจอในการใช้สมาร์ตโฟนอยู่เสมอ แชรข้อมูลส่วนตัวในโซเชียลมีเดียอย่างระมัดระวัง ใส่ใจกับการตั้งค่าความเป็นส่วนตัว ไม่ควรใช้ Wi-Fi สาธารณะเมื่อต้องกรอกข้อมูลส่วนตัว และรู้ทันภัยคุกคามทางอินเทอร์เน็ต

(3.5) ทักษะในการจัดสรรเวลาหน้าจอ (Screen Time Management) ไม่ว่าจะเป็นเวลาที่ใช้คอมพิวเตอร์ แท็บเล็ต โทรศัพท์มือถือ การเข้าสังคมออนไลน์ และการดูโทรทัศน์

(3.6) ทักษะในการบริหารจัดการข้อมูลของผู้ใช้งานมีทั้งไว้บนโลกออนไลน์ (Digital Footprints)

(3.7) ทักษะในการรับมือการกลั่นแกล้งบนโลกออนไลน์ (Cyberbullying Management) จะครอบคลุมการว่าร้าย ใส่ความ ช่มชู้ ทำร้าย หรือใช้ถ้อยคำหยาบคาย การ Blackmail การหลอกลวง การคุกคามทางเพศผ่านสื่อออนไลน์ การแอบอ้างตัวตนผู้อื่น และการสร้างกลุ่มโซเชียลเพื่อโจมตีโดยเฉพาะสำหรับวิธีการจัดการเมื่อถูกกลั่นแกล้งบนโลกไซเบอร์ คือ หยุดการตอบโต้ บล็อกการปิดกั้น และแจ้งให้ทราบ

ส่วนที่ 2 (ต่อ)

2.1 รายงานสรุปเนื้อหา (ต่อ)

(3.8) ทักษะในการใช้เทคโนโลยีอย่างมีจริยธรรม (Digital Empathy) ก่อนทำอะไรลงบนโลกออนไลน์ควรจะคิดก่อนโพสต์ ควรใคร่ครวญก่อนที่จะโพสต์รูปหรือข้อความลงบนสื่อออนไลน์ ไม่ว่าจะโพสต์อยู่ในขณะที่มีอารมณ์โกรธ การสื่อสารกับผู้อื่นด้วยเจตนาดี ไม่ใช่จากที่สร้างความเกลียดชังทางออนไลน์ ไม่ล่วงข้อมูลส่วนตัวของผู้อื่น ไม่กลั่นแกล้งผู้อื่นผ่านสื่อดิจิทัล โดยตั้งคำถามกับตนเองก่อนว่าควรโพสต์หรือไม่

3.2) อัตลักษณ์ดิจิทัล (Digital Identity)

(1) โลกดิจิทัล (Digital World) คือ โลกเสมือนที่ถูกสร้างขึ้นคู่ขนานกับโลกความเป็นจริง เป็นเครื่องมือทรัพยากร มีกิจกรรมคล้ายกับโลกความเป็นจริง พื้นที่ในโลกดิจิทัลถูกสร้างขึ้นจากอุปกรณ์อิเล็กทรอนิกส์ที่สามารถกำหนดพื้นที่กิจกรรมต่าง ๆ ได้ เหมือนกับโลกความเป็นจริง ใช้ในการเป็นพื้นที่พูดคุย แลกเปลี่ยนประสบการณ์ สามารถใช้โซเชียลมีเดียได้ พื้นที่ในการซื้อขายสินค้าและธุรกรรมทางการเงิน ร้านค้าออนไลน์หรือธนาคารออนไลน์ โลกพื้นที่ในกิจกรรมโลกดิจิทัลนั้นจะมีเฉพาะสมาชิกหรือผู้คนพลเมืองดิจิทัลเท่านั้น เช่น โปรแกรม Spatial ซึ่งสามารถสร้างโลกจำลองเสมือนจริง

(1.1) การเปรียบเทียบโลกดิจิทัลและโลกความเป็นจริง แบ่งเป็น

- การค้นหาและเข้าถึงสื่อที่ต้องการ
โลกดิจิทัล: เข้าถึงได้สะดวกกว่าด้วยอุปกรณ์พกพา นำสื่อมาใช้ได้ง่ายสะดวกทุกที่ทุกเวลา
โลกความเป็นจริง: มีข้อจำกัดการเข้าถึงต้องเดินทางไปยังที่เก็บข้อมูล ต้องรอข่าวสารจากสื่อ
- การพูดคุย การติดต่อกับผู้คนที่ไม่ค่อยได้พบกัน
โลกดิจิทัล: ทำได้อย่างรวดเร็ว สามารถส่งข้อความในแอปพลิเคชัน หากมีเรื่องด่วนสามารถโทรด้วยภาพและเสียง
โลกความเป็นจริง: ต้องรอให้ว่างตรงกัน ต้องอยู่ในสถานที่เดียวกัน มีข้อจำกัดในการพูดคุย
- การเผยแพร่สื่อ เนื้อหา และบอกเล่าประสบการณ์
โลกดิจิทัล: ใช้โซเชียลมีเดียโพสต์แบ่งปันความรู้สึก เผยแพร่รูปภาพ วิดีโอที่เป็นประโยชน์กับผู้อ่าน
โลกความเป็นจริง: อาจจะมีข้อจำกัดการเผยแพร่ด้วยการบอกเล่า รับรู้ได้แค่บุคคลใกล้ชิด เช่น ครอบครัว เพื่อน เป็นต้น
- การให้คำปรึกษา สร้างแรงบันดาลใจ
โลกดิจิทัล: ทำได้ไม่ค่อยดีเพราะอาศัยการพิมพ์ ความรู้สึกไม่สามารถถ่ายทอดได้อย่างเต็มที่
โลกความเป็นจริง: ได้เห็นหน้า มองตา สัมผัสกาย เกิดความเข้าใจ ทั้งในด้านเนื้อหาและอารมณ์
- การร่วมกิจกรรมที่อาศัยการปฏิบัติ
โลกดิจิทัล: อาจทำได้ในบางเรื่องที่ไม่ซับซ้อน
โลกความเป็นจริง: อาศัยผู้เชี่ยวชาญหรือผู้มีประสบการณ์ การปฏิบัติมีประสิทธิภาพมากกว่า เช่น การฝึกทำขนม
- การทำธุรกรรมของภาครัฐในบางประเภท
โลกดิจิทัล: มีการทำผ่านระบบดิจิทัล เช่น การเงิน ต้องไปทำในโลกจริงบางส่วน เช่น โอนที่ดิน ทำใบขับขี่
โลกความเป็นจริง: ทำธุรกรรมได้ทุกประเภทหากเดินทางไปทำการ

ส่วนที่ 2 (ต่อ)

2.1 รายงานสรุปเนื้อหา (ต่อ)

(1.2) มารยาทในโลกดิจิทัล สำหรับสิ่งที่ควรทำ คือ ใส่ใจให้เกียรติผู้อื่น แบ่งปันสิ่งดี ๆ และสร้างสรรค์ ตรวจสอบการส่งต่อข้อมูลให้ตรงกับกลุ่มเป้าหมาย ปฏิบัติตามกฎหมายของชุมชนและโลกออนไลน์ และสำหรับสิ่งที่ไม่ควรทำ คือ การแสดงความคิดเห็นด้วยถ้อยคำรุนแรง แสดงอารมณ์ขันที่หมิ่นเหม่เสียดสี ส่งต่อข้อมูลที่ไม่น่าเชื่อว่าเป็นความจริงหรือไม่ และใช้โซเชียลมีเดียในการให้ร้ายผู้อื่น

(2) จริยธรรมของพลเมือง คือ ความเข้าใจการปฏิบัติที่เกิดขึ้นในสังคมดิจิทัลที่น่าอยู่ ได้แก่ การให้เกียรติ เคารพความคิดเห็นและสิทธิของผู้อื่น หลีกเลี่ยงการระราน ข่มขู่ หรือหยอกล้อเกินพอดี ขออนุญาตเมื่อนำข้อมูลผู้อื่นไปใช้ ไตร่ตรองก่อนแชร์หรือโพสต์ข้อมูล ไม่ควรแชร์หรือโพสต์ข้อมูลส่วนบุคคลมากเกินไป ระวังการแชร์หรือโพสต์ข้อมูล หลีกเลี่ยงการแท็กภาพหรือข้อมูลถึงผู้อื่น และระวังการใช้ความเป็นผู้อาวุโสในการสนทนา

(3) ความเป็นส่วนตัวในโลกดิจิทัล (Digital Privacy)

(3.1) ข้อมูลที่สามารถเผยแพร่ได้ไม่เป็นอันตราย เช่น ชื่อจริง ชื่อเล่น อายุ เพศ พี่น้อง อาหารที่ชอบ หนังสือเรื่องโปรด เป็นต้น และข้อมูลส่วนบุคคลที่ไม่ควรเปิดเผยเป็นสาธารณะ เนื่องจากความปลอดภัย ทั้งตัวตนบนโลกดิจิทัลและชีวิตจริง ควรเก็บไว้เป็นส่วนตัว เช่น เลขบัตรประชาชน เลขบัญชีธนาคาร ที่อยู่บ้าน วันเกิด หมายเลขโทรศัพท์ เป็นต้น

(3.2) การจัดการข้อมูลส่วนตัว ไม่เปิดเผยหรือเผยแพร่ข้อมูลที่ไม่ควรเปิดเผย หลีกเลี่ยงการตั้งโปรไฟล์โซเชียลมีเดียให้เป็นสาธารณะ การจัดการอุปกรณ์ให้ปลอดภัย ทำความเข้าใจเงื่อนไขข้อตกลงโดยใช้

โปรแกรม หรือ Application และตั้งรหัสผ่านให้มีความปลอดภัย

(3.3) กฎหมายที่เกี่ยวข้องกับสิทธิและความเป็นส่วนตัวบนโลกดิจิทัล ได้แก่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ซึ่งมีบทลงโทษผู้ละเมิดสิทธิและความเป็นส่วนตัวของโลกดิจิทัล ดังนี้

- โทษทางอาญาจำคุกไม่เกิน 1 ปี และปรับสูงสุด 1 ล้านบาท
- โทษทางแพ่งจ่ายสินไหมไม่เกิน 2 เท่าของสินไหมที่แท้จริง
- โทษทางการปกครองปรับไม่เกิน 5 ล้านบาท

(3.4) บทลงโทษของผู้ละเมิดอัตลักษณ์ทางด้านดิจิทัลและความเป็นส่วนตัวตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ. 2550 และ ปี พ.ศ. 2560 ดังนี้

- แก้ไขตัดแปลงหรือทำให้ข้อมูลผู้อื่นเสียหาย (มาตรา 9 และมาตรา 10) จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ
- ส่งข้อมูลหรืออีเมลก่อนผู้อื่นหรือส่งอีเมลสแปม (มาตรา 11) ปรับไม่เกิน 100,000 บาท
- นำข้อมูลที่ผิด พ.ร.บ. เข้าสู่ระบบคอมพิวเตอร์ (มาตรา 14) โทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

หากเป็นการกระทำที่ส่งผลต่อบุคคลใดบุคคลหนึ่ง โทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ

(3.5) ปัญหาที่เกิดจากภาวะคุกคามและละเมิดความเป็นส่วนตัว ได้แก่ การละเมิดข้อมูลส่วนตัวจากการใช้แอปพลิเคชัน การหลอกลวงด้วยความจริงเพียงครั้ง การหลอกลวงข้อมูลเป็นประเด็นที่อ่อนไหว และการละเมิดหรือใช้ข้อมูลส่วนตัวที่ผิดวัตถุประสงค์ของภาครัฐกิจ

(3.6) การป้องกันการถูกคุกคามความเป็นส่วนตัวในโลกดิจิทัล โดยการสร้างรหัสผ่านที่รัดกุม อัปเดตระบบอยู่ตลอด ตั้งค่าความปลอดภัยบนอุปกรณ์ ป้องกันอุปกรณ์ด้วยซอฟต์แวร์ป้องกันไวรัส และสำรองไฟล์ข้อมูลไปยังคลาวด์หรือบนฮาร์ดไดรฟ์ภายนอก

ส่วนที่ 2 (ต่อ)

2.1 รายงานสรุปเนื้อหา (ต่อ)

3.3) การใช้เทคโนโลยีดิจิทัลอย่างเหมาะสม (Digital Use)

(1) การใช้เทคโนโลยีอย่างสมดุล ซึ่งเวลาในการใช้หน้าจอก็จะมีผลต่อร่างกายและการใช้ชีวิต เช่น ปวดหลัง ปวดคอ ผลเสียต่อสายตา นิ้วล็อค และหากใช้งานในระยะเวลาเกินไปจะทำให้เกิดความเครียด โดยหลักเกณฑ์ในการใช้หน้าจอที่เหมาะสม คือ มีเป้าหมายทุกครั้งที่ใช้งานดิจิทัล ใช้ร่างกายเป็นมาตรวัด เตรียมใจเมื่อพร้อมที่จะใช้เวลาเจอเจอ สำหรับเครื่องมือที่ใช้ในการบริหารจัดการหน้าจอมีคือระบบ Android คือแอปพลิเคชัน Digital Wellbeing เพื่อดูเวลาในการใช้หน้าจอ และมือถือระบบ IOS ให้ไปที่ตั้งค่า เลือกเวลาหน้าจอ สำหรับการใช้โทรศัพท์มือถืออย่างไรไม่เสียต่อสุขภาพ เช่น เวลาใช้โทรศัพท์มือถือต้องห่างจากสายตา ประมาณ 12-15 นิ้ว ยกจอตั้งคอกกับลำตัว ควรนั่งเล่นบนอุปกรณ์ที่มีเก้าอี้พนักพิงประมาณ 100 องศา ไม่ควรเล่นติดต่อกันเกิน 1-2 ชั่วโมง พักสายตาและข้อมืออย่างน้อย 5-10 นาทีต่อชั่วโมง ควรปรับหน้าจอให้สว่างตามสภาพแสง ทั้งนี้ในส่วนของการเสพติดเนื้อหาหรือเสพติดอินเทอร์เน็ตอาจส่งผลต่อสุขภาพจิต ดังนี้ เกิดภาวะซึมเศร้า เสียต่ออาการวิตกกังวล ขาดความยับยั้งชั่งใจ หรือรู้สึกต่อต้านสังคม สำหรับการตั้งค่าเนื้อหาที่เหมาะสมในการใช้งานแพลตฟอร์ม โดยใช้ Google Chrome ให้ไปที่จุดสามจุดด้านบน จากนั้นไปที่ตั้งค่า แล้วเลือกเครื่องมือการค้นหา เลือกการจัดการเครื่องมือค้นหาบนเว็บไซต์ และสามารถกรองเนื้อหาได้ว่าเราสามารถใช้ตัวของเว็บเบราว์เซอร์ค้นหาข้อมูลแบบใด

(2) การเอาใจเขามาใส่ใจเราทางดิจิทัล เช่น กรณีคนใกล้ชิดโพสต์ข้อความสั้นหวังหมุดกำลังใจในการทำงาน ซึ่งสิ่งที่ควรทำ คือ แสดงความเห็นอย่างจริงใจตรงไปตรงมา เช่น เป็นกำลังใจให้นะ มีอะไรให้ช่วยบอกนะ ส่งสติ๊กเกอร์ห่วยๆ และตระหนักเสมอว่าไม่เพียงแค่ว่าเราเป็นผู้สื่อสารกับคนนั้นแต่ยังมีอีกหลายคนที่เป็นเพื่อนเขา ควรระมัดระวังก่อนที่จะแสดงความคิดเห็น และสิ่งที่ไม่ควรทำ คือ แสดงความเห็นหยอกล้อ ความรู้สึกสนุกสนาน เนื่องจากตัวหนังสือไม่มีน้ำเสียงและความรู้สึก อาจจะตีความหมายการสื่อสารผิดได้ สำหรับข้อระวังเนื้อหาในการโพสต์ คือ เนื้อหาหรือรูปภาพเป็นลิขสิทธิ์ของผู้อื่น ก่อให้เกิดความขัดแย้งทางด้านความเชื่อและศาสนา แสดงเนื้อหาความรุนแรงและทารุณ และแอบอ้างภาพบุคคลอื่นที่ไม่ได้รับอนุญาต

3.4) การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security)

(1) การล่วงละเมิดทางไซเบอร์ คือ การแสดงพฤติกรรมที่เป็นอันตราย สร้างความรำคาญหรือสร้างความเสียหายให้กับผู้อื่นบนเครือข่ายออนไลน์ต่าง ๆ ทั้งด้านความรู้สึก หรืออาจลุกลามไปยังทรัพย์สินหรือการละเมิดในชีวิตจริงในการใช้โซเชียลมีเดีย เกมส์ เครือข่ายออนไลน์ ได้แก่ การระรานทางไซเบอร์ การรังควานทางไซเบอร์ การสะกดรอยตามทางไซเบอร์ และการก่อกวน สาเหตุในการล่วงละเมิดทางไซเบอร์ คือ ต้องการก่อกวนโดยไม่มีสาเหตุ ต้องการกลั่นแกล้ง ต้องการรังควานผู้เป็นเป้าหมายหรือผู้ที่ขัดแย้งอยู่ ต้องการข่มขู่สร้างความหวาดกลัวผู้ที่ตกเป็นเป้าหมาย หรือติดตามไปประสังครายในชีวิตจริง

(2) สาเหตุภัยคุกคามทางไซเบอร์ (Cyber Threat) คือ

(2.1) การตั้งพาสเวิร์ดที่ง่ายเกินไป เช่น การตั้งรหัส 123456 นับล้านบัญชี เนื่องจากจำง่าย ซึ่ง Password ยอดนิยมทั่วโลก 5 ลำดับแรก (ค.ศ. 2022) คือ password, 123456, 123456789, quest, qwerty

(2.2) โปรแกรมรักษาความปลอดภัยไม่ทำงาน เช่น อาจจะมีมัลแวร์หรือขาดการอัปเดต โปรแกรมอย่างสม่ำเสมอ ซึ่งเป็นช่องโหว่ให้ผู้ประสงค์ร้ายเข้ามาขโมยข้อมูลหรือสร้างความเสียหายให้กับข้อมูล

(2.3) ความประมาท ซึ่งผู้ที่ไม่ระมัดระวังหรือประมาทกดรับไฟล์หรือลิงก์จากผู้อื่นที่ไม่รู้จัก

ส่วนที่ 2 (ต่อ)

2.1 รายงานสรุปเนื้อหา (ต่อ)

(3) รูปแบบของภัยคุกคามทางไซเบอร์ คือ

(3.1) อีเมลอันตราย อีเมลที่เหมือนมาจากเกมส์ หรืออื่น ๆ หากกดรับบัญชีจะถูกบุกรุกเพื่อให้ได้ข้อมูลส่วนบุคคลหรือเสียทรัพย์สิน

(3.2) สปแอม (Spam) อีเมลที่มีข้อความที่ส่งให้ผู้รับโดยไม่ได้รับอนุญาตและไม่เปิดโอกาสให้ปฏิเสธข้อความ ซึ่งก่อให้เกิดความรำคาญ

(3.3) ฟิชซิง (Phishing) การหลอกลวงให้เหยื่อคลิก หรือให้เหยื่อกรอกข้อมูลส่วนตัว คำว่า ฟิชซิงคล้ายการตกปลา เพื่อล่อเหยื่อ

(3.4) มัลแวร์ (Malware) โปรแกรมที่สร้างความเสียหายต่ออุปกรณ์ไอที ตั้งแต่การเข้าควบคุมระบบคอมพิวเตอร์ เปลี่ยนรหัสผ่าน แก้ไขข้อมูลต่าง ๆ รวมถึงเรียกค่าไถ่

(3.5) ภัยจากการขอบังคับออนไลน์ มักเป็นช่องทางสำหรับผู้ไม่หวังดี

(3.6) ภัยจากการไม่สำรองข้อมูล การจัดเก็บข้อมูลทั้งหมดไว้บนคอมพิวเตอร์มีความเสี่ยงที่จะสูญหาย

3.5 การรู้เท่าทันดิจิทัล (Digital Literacy)

(1) การใช้งานสื่อสารสนเทศ โดยแหล่งข้อมูลดิจิทัล คือ แหล่งข้อมูลที่ถูกสร้างขึ้นหรือแปลงสภาพจากอนาล็อกให้มาเป็นในรูปแบบของดิจิทัล ซึ่งสามารถค้นหา เข้าถึง นำเข้าข้อมูลผ่านระบบอินเทอร์เน็ต เช่น เว็บไซต์ที่ทำให้ดูข้อมูลด้านสุขภาพ ข่าวสาร หรือบทความต่าง ๆ เป็นต้น

(1.1) รูปแบบของแหล่งข้อมูลดิจิทัลสามารถแบ่งได้ดังนี้

- แบ่งตามแหล่งที่เผยแพร่ข้อมูล (เจ้าของแหล่งข้อมูล/ชุมชนผู้ใช้งาน)
- แบ่งตามสิทธิ์การเข้าถึงข้อมูล (เข้าถึงโดยเสรี/จำกัดการเข้าถึง)
- แบ่งประเภทตามข้อมูล (การศึกษา/ความบันเทิง/สุขภาพ/ธุรกรรมการเงิน/เศรษฐศาสตร์)

(1.2) สำหรับลักษณะข้อมูลที่มีคุณภาพ คือ ทันสมัยตอบโจทย์ เทียบตรง แม่นยำ ผู้เขียนเชื่อถือได้

(1.3) ผลจากการแบ่งปันเนื้อหาที่ไม่เหมาะสม แบ่งเป็น

การกระทำ/พฤติกรรม	ผลกระทบทางกฎหมาย	ผลกระทบทางจริยธรรม
ฝากร้าน ขายของ และส่งข้อความ ก่อกวน โดยไม่ได้รับอนุญาต	มีความผิดปรับไม่เกิน 2 แสนบาท	ทำให้ผู้อื่นเกิดความรำคาญ
โพสต์หรือแชร์ข้อมูลเท็จที่สร้างความเสียหายต่อบุคคลหรือประเทศ	จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 1 แสนบาท และระงับข้อมูลนั้น	เกิดความเข้าใจผิดและอับอาย สร้างความเกลียดชัง ทำให้เสียชื่อเสียง
โพสต์ข้อความปลอม ข้อมูลทุจริต หลอกลวง ที่สร้างความเสียหายต่อความมั่นคง	จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท และระงับข้อมูลนั้น หรือลงโทษตามมาตรา	เกิดจากความตื่นตระหนก การขัดแย้งทางสังคม ทำให้ตัดสินใจผิดพลาดได้
โพสต์หรือแชร์ข้อมูลภาพตัดต่อที่สร้างความเสี่ยงต่อผู้อื่น	จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 2 แสนบาท และระงับข้อมูลนั้น	สร้างความอึดอัด ความสะเทือนใจ และความรู้สึกหตุ

ส่วนที่ 2 (ต่อ)

2.1 รายงานสรุปเนื้อหา (ต่อ)

(2) ผู้จัดทำสื่อและสารสนเทศ โดยประเภทของเนื้อหาดิจิทัล แบ่งเป็น สุขภาพอนามัย ข้อมูลภาครัฐ ด้านความบันเทิง ด้านการตลาด ด้านการศึกษาและเรียนรู้ และด้านข่าวสาร

(2.1) ประเภทของสื่อดิจิทัล เป็นสื่อที่สร้างขึ้นมาเพื่อบันทึกเหตุการณ์เรื่องราว อาจเป็นภาพถ่ายหรือภาพสแกน ข้อความดิจิทัลสร้างขึ้นเพื่อบอกเล่าเหตุการณ์ผลิตโดยโปรแกรมคอมพิวเตอร์ เสียงสร้างขึ้นสำหรับการบรรยายโดยใช้อุปกรณ์บันทึกเสียงหรือโปรแกรมคอมพิวเตอร์ วิดีโอเป็นการผสมของเสียงและภาพสร้างด้วยโทรศัพท์หรือกล้องวิดีโอ ภาพกราฟิกดิจิทัลเป็นการสร้างภาพแทนความหมายต่าง ๆ เพื่อให้เกิดความเข้าใจข้อมูลที่ซับซ้อน เช่น กราฟ แผนภูมิ อินโฟกราฟิก เป็นต้น

(2.2) หลักการสร้างเนื้อหาให้ถูกกฎหมายและมีจริยธรรม แบ่งเป็น

- ลิขสิทธิ์แบบเดิม ห้ามทุกคน ห้ามทุกอย่าง เป็นกรอบแนวคิดของสมัยเดิม ก่อนเกิดเทคโนโลยีสารสนเทศ และแลกเปลี่ยนข้อมูลผ่านอินเทอร์เน็ต

- Creative Commons เสนอทางเลือกที่เจ้าของลิขสิทธิ์สามารถแบ่งปันข้อมูลได้ เลือกสงวนสิทธิ์ตามที่ต้องการได้ ตรงใจ ตรง Lifestyle

(2.3) ประเภทรูปแบบ Creative Commons (CC license) มีดังนี้

- Attribution (BY) ยอมให้แจกจ่ายเปลี่ยนแปลง ดัดแปลงหรือใช้งานต้นฉบับอย่างใดอย่างหนึ่ง รวมถึงการค้า และต้องมีอ้างอิง

- Share Alike (SA) ยอมให้เปลี่ยนแปลง ดัดแปลง รวมถึงการค้า และต้องมีอ้างอิง

- Non-Commercial (NC) ยอมให้ใช้และแจกจ่ายต่อ รวมถึงการค้า และต้องมีอ้างอิง แต่ห้ามดัดแปลง

- No Derivative Works (ND) ยอมให้เปลี่ยนแปลง ดัดแปลง และต้องมีอ้างอิง แต่ห้าม

ใช้ทางการค้า

3.6 การสื่อสารดิจิทัล (Digital Communication)

(1) ร่องรอยดิจิทัล (Digital Footprint) ข้อมูลพฤติกรรมการใช้งานในโลกดิจิทัล ซึ่งระบบจะบันทึกไว้ทั้งหมด โดยเกิดขึ้นจากการใช้งาน ไม่ว่าจะเป็นการค้นหาข้อมูล ค้นหาสินค้าและบริการ การใช้งานโซเชียลมีเดียต่าง ๆ ทั้งโพสต์ คอมเมนต์ และแชร์เนื้อหา หรือการพูดคุยทางแชท สำหรับเครื่องมือช่วยจัดการร่องรอยดิจิทัล คือ แอปจัดการรหัสผ่าน (ดูผลการชิงครหัสผ่านกับบัญชีต่าง ๆ และแจ้งเตือนเมื่อรหัสผ่านรั่วไหล เช่น Dropbox Passwords, 1Passwords, Chrome Password Manager เป็นต้น) แอปหรือเว็บไซต์ช่วยป้องกันการติดตาม (จะช่วยป้องกันการติดตามและบันทึกการใช้งานต่าง ๆ ป้องกันไม่ให้ข้อมูลรั่วไหล เช่น Disconnect, Ghostery เป็นต้น) เครื่องมือค้นหาแบบส่วนตัว (เครื่องมือเหล่านี้จะช่วยให้ค้นหาสิ่งที่ต้องการแบบไม่เปิดเผยตัวตน เช่น Startpage, Disconnect Search, DuckDuckGo เป็นต้น)

(2) การมีปฏิสัมพันธ์และการสร้างความร่วมมือ ได้แก่ การสื่อสารระหว่างบุคคล (เป็นการใช้เทคโนโลยีดิจิทัลสื่อสาร เช่น โทรศัพท์ พิมพ์ข้อความ คอลหรือวิดีโอคอลในห้องสนทนา) การสื่อสารระหว่างกลุ่มคนเฉพาะกลุ่มแบบไม่เป็นสาธารณะ (ใช้ตั้งกลุ่มเพื่อการสื่อสาร เช่น กลุ่มเฟซบุ๊กที่เป็นกลุ่มปิด หรือกลุ่มสนทนาในโซเชียลมีเดีย) และการสื่อสารระหว่างกลุ่มคนแบบเป็นสาธารณะ (การใช้โพสต์แบบเป็นสาธารณะ เช่น โพสต์บนหน้าเฟซบุ๊กส่วนตัวแล้วเปิดเป็นสาธารณะ ตั้งกลุ่มเฟซบุ๊กแบบสาธารณะ ตั้งกลุ่มในไลน์แบบเปิด)

ส่วนที่ 2 (ต่อ)

2.2 ประสบการณ์/ประโยชน์ที่ได้รับ/การประยุกต์ใช้กับหน่วยงาน

ต่อตนเอง/ต่อหน่วยงาน

หลักสูตรนี้ช่วยทำให้เข้าใจความหมาย และเห็นความสำคัญการสร้างความรู้ในการใช้อินเทอร์เน็ต รู้เท่าทันและมีความมั่นคงปลอดภัย อีกทั้งสามารถนำเทคโนโลยีดิจิทัลมาปรับใช้ในการปฏิบัติงานหรือพัฒนางานให้มีประสิทธิภาพมากยิ่งขึ้น

2.3 ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ -

2.4 ข้อคิดเห็น -

ลงชื่อ ไอลษา บุญเลิศ

(นางสาวไอลษา บุญเลิศ)

ตำแหน่ง เศรษฐกรชำนาญการพิเศษ

ผู้รายงาน

วันที่ 9 เดือน กุมภาพันธ์ พ.ศ. 2569

ส่วนที่ 3 ความเห็นของผู้บังคับบัญชา

ทราบ

ลงชื่อ [ลายเซ็น]

(นายบัณฑิต หนองหารพิทักษ์)

ตำแหน่ง ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่ 10 เดือน กพ พ.ศ. 2569

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ วัลยา บุญเลิศ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Digital Literacy : ความฉลาดทางดิจิทัล
(Digital Intelligence)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 31 มกราคม 2569

สำเนาถูกต้อง

โสภา บุญเลิศ

(นางสาววัลยา บุญเลิศ)
เศรษฐกรชำนาญการพิเศษ

Ah.

(นางโอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ วัลยา บุญเลิศ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
(Digital Government Act.)

จำนวนชั่วโมงการเรียนรู้ 0:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 31 มกราคม 2569

สำเนาถูกต้อง

วัลยา บุญเลิศ
(นางสาววัลยา บุญเลิศ)
เศรษฐกรชำนาญการพิเศษ

Ah

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

