

**สรุปบทเรียนการพัฒนาความรู้
หลักสูตร ความฉลาดทางดิจิทัล
(Digital Intelligence / Digital Literacy)**

ชื่อ-สกุล (ภาษาไทย) : นางอมรรัตน์ อุปแก้ว ตำแหน่ง: เจ้าพนักงานการเกษตรชำนาญงาน

สังกัด: กลุ่มวิจัยเคมีดิน สำนักวิทยาศาสตร์เพื่อการพัฒนาที่ดิน

วันที่อบรม: 8 เมษายน 2569

วัตถุประสงค์ของหลักสูตร

1. ใช้เทคโนโลยีเพื่อการเรียนรู้และพัฒนา
2. ใช้เทคโนโลยีอย่างปลอดภัย
3. ใช้อย่างมีจริยธรรมและความรับผิดชอบ ไม่เผยแพร่ข้อมูลเท็จ หรือเนื้อหาที่ไม่เหมาะสม
4. เพื่อให้คน ใช้ดิจิทัลอย่างฉลาด ปลอดภัย มีคุณธรรม และเกิดประโยชน์สูงสุด ทั้งต่อตนเองและสังคม

สรุปบทเรียน

ความฉลาดทางดิจิทัล (Digital Intelligence หรือ Digital Literacy)

เกิดขึ้นจากการเปลี่ยนแปลงของโลกในยุคเทคโนโลยีสารสนเทศและการสื่อสาร โดยในยุคเริ่มต้นของเทคโนโลยีก่อนปี 1990 ในช่วงนี้คอมพิวเตอร์ยังมีขนาดใหญ่และใช้งานเฉพาะองค์กร หรือหน่วยงานสำคัญ ทักษะที่จำเป็นคือ การรู้จักใช้คอมพิวเตอร์พื้นฐาน เช่น การพิมพ์ การจัดเก็บข้อมูล ยังไม่เรียกว่าความฉลาดทางดิจิทัล แต่เป็นจุดเริ่มของความรู้ด้านคอมพิวเตอร์ยุคอินเทอร์เน็ตเริ่มแพร่หลาย ประมาณปี 1990-2000 อินเทอร์เน็ตเริ่มเข้ามา มีบทบาท ทำให้เกิดการสื่อสารออนไลน์ เช่น อีเมล เว็บไซต์ แนวคิด Digital Literacy เริ่มถูกใช้ หมายถึง การค้นหาข้อมูล การประเมินข้อมูล การใช้อินเทอร์เน็ตอย่างถูกต้อง ยุคโซเชียลมีเดียและสมาร์ทโฟน 2000-ปัจจุบัน เทคโนโลยีเข้าถึงทุกคนผ่านมือถือและโซเชียลมีเดีย เช่น Facebook Instagram LINE ทำให้เกิดความจำเป็นใหม่ เช่น การคิดวิเคราะห์ข่าวสาร (Fake News) การปกป้องข้อมูลส่วนตัว มารยาททางดิจิทัล ยุคดิจิทัลเต็มรูปแบบ ปัจจุบันโลกเข้าสู่สังคมดิจิทัลเต็มรูปแบบ ทั้งการเรียน การทำงาน และการใช้ชีวิตประจำวัน

ความฉลาดทางดิจิทัลจึงครอบคลุม 3 ด้านหลัก ได้แก่

1. ทักษะ (Skills) – การใช้เทคโนโลยีอย่างมีประสิทธิภาพ
2. ความรู้ (Knowledge) – เข้าใจสื่อและข้อมูล
3. คุณธรรม (Ethics) – ใช้อย่างปลอดภัย มีความรับผิดชอบ

ความฉลาดทางดิจิทัล หมายถึง ความสามารถในการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ ปลอดภัย และมีความรับผิดชอบ รวมถึงการรู้เท่าทันสื่อ การคิดวิเคราะห์ข้อมูล และการปฏิบัติตนอย่างเหมาะสมในโลกออนไลน์ ประกอบด้วยองค์ประกอบสำคัญของความฉลาดทางดิจิทัล 8 ด้านหลัก ดังนี้

1. อัตลักษณ์ดิจิทัล (Digital Identity) คือ ภาพลักษณ์ ตัวตน และข้อมูลของเราที่ปรากฏอยู่บนโลกออนไลน์ ซึ่งเกิดจากการใช้งานอินเทอร์เน็ตและสื่อดิจิทัล เช่น โซเชียลมีเดีย อีเมล หรือเว็บไซต์ต่าง ๆ ควรสร้างให้ดี เพราะส่งผลต่อภาพลักษณ์ในระยะยาว อาทิ รอยเท้าดิจิทัล (Digital Footprint) คือ ข้อมูล หรือร่องรอยต่าง ๆ ที่เราทิ้งไว้ บนโลกออนไลน์จากการใช้งานอินเทอร์เน็ตแบบตั้งใจ เช่น โพสต์เอง และแบบไม่ตั้งใจ เช่น เว็บไซต์เก็บข้อมูล พฤติกรรมการใช้งานโดยอัตโนมัติ ทำให้ถึงสำคัญ เพราะข้อมูลเหล่านี้ อาจถูกนำไปใช้พิจารณา เช่น การสมัครงาน อาจส่งผลต่อภาพลักษณ์และความน่าเชื่อถือ ถ้าไม่ระวังอาจกระทบความเป็นส่วนตัว

วิธีดูแล Digital Footprint คิดก่อนโพสต์ทุกครั้ง ตั้งค่าความเป็นส่วนตัวในโซเชียล ไม่เปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน ตรวจสอบประวัติออนไลน์ของตนเองเป็นระยะ

องค์ประกอบของอัตลักษณ์ดิจิทัล ข้อมูลส่วนตัว เช่น ชื่อ รูปภาพ วันเกิด พฤติกรรมออนไลน์ เช่น การโพสต์ แสดงความคิดเห็น การกดไลก์ ผลงาน/เนื้อหา ที่เราแชร์ เช่น รูป วิดีโอ หรือบทความ ประวัติการใช้งาน เช่น การค้นหา หรือการเข้าชมเว็บไซต์

ความสำคัญของอัตลักษณ์ดิจิทัล สร้างภาพลักษณ์และความน่าเชื่อถือ มีผลต่อโอกาสการเรียนรู้ และการทำงาน เป็นสิ่งที่คนอื่นใช้ในการ ตัดสินตัวตนของเรา

แนวทางการสร้างอัตลักษณ์ดิจิทัลที่ดี คิดก่อนโพสต์หรือแชร์ข้อมูล ใช้ถ้อยคำสุภาพ มีมารยาท ไม่เผยแพร่ข้อมูลเท็จหรือเนื้อหาที่ไม่เหมาะสม ตั้งค่าความเป็นส่วนตัวให้เหมาะสม สร้างคอนเทนต์ที่เป็นประโยชน์และสร้างสรรค์

2. การใช้ดิจิทัลหรือการใช้เทคโนโลยีอย่างเหมาะสม (Digital Use) และการใช้เทคโนโลยีอย่างสมดุล (Balanced Use) เป็นทักษะสำคัญของการเป็นพลเมืองดิจิทัลที่ดี มีแนวคิดหลัก ดังนี้

2.1 การใช้เทคโนโลยีอย่างเหมาะสม (Appropriate Digital Use) คือ การใช้เทคโนโลยีอย่างถูกต้อง มีจริยธรรม และเกิดประโยชน์สูงสุด

2.2 การใช้เทคโนโลยีอย่างสมดุล (Balanced Digital Use) คือ ควบคุมเวลา และพฤติกรรมการใช้เทคโนโลยีให้พอดี ไม่มากเกินไปจนกระทบชีวิต แนวทางปฏิบัติ กำหนดเวลาใช้งาน เช่น ไม่ใช้มือถือก่อนนอน หลีกเลี่ยงการใช้หน้าจอต่อเนื่องเป็นเวลานาน พักสายเป็นระยะ เช่น กฎ 20-20-20 ลดพฤติกรรมติดโซเชียล หรือเกมมากเกินไป โดยทั่วไปการใช้โทรศัพท์มือถือ ควรถือให้อยู่ระดับเดียวกับสายตา และห่างจากตาประมาณ 12-18 นิ้ว เพื่อป้องกันอาการเมื่อยล้าของสายตา ลดความเสี่ยงสายตาสั้น ป้องกันอาการปวดคอจากการก้มมองหน้าจอ

3. ความปลอดภัยทางดิจิทัล (Digital Safety) การป้องกันตนเองจากภัยออนไลน์ เช่น ไวรัส แสกเกอร์ หรือ การหลอกลวง (Phishing)

การหลอกลวง (Phishing) คือ การหลอกลวงผ่านอีเมล ข้อความ หรือเว็บไซต์ปลอม เพื่อให้เหยื่อกรอกข้อมูลสำคัญ เช่น รหัสผ่าน เลขบัตรประชาชน หรือข้อมูลธนาคาร โดยแอบอ้างเป็นหน่วยงานที่น่าเชื่อถือ เช่น ธนาคาร หรือแอปต่าง ๆ ข้อมูลที่ระบุตัวตนได้ชัดเจน หรือเกี่ยวกับการเงินและความปลอดภัย ไม่ควรเปิดเผยในโลกดิจิทัล คือ รหัสผ่านหรือข้อมูลทางการเงิน การป้องกันการถูกคุกคามบนอุปกรณ์ตนเอง โดยการตั้งรหัสผ่านที่คาดเดายาก หรือตั้งรหัสผ่านที่รัดกุม ไม่กดลิงก์แปลก ๆ อัปเดตแอป และระบบสม่ำเสมอ

รหัสผ่านที่มีความปลอดภัยควรมีลักษณะดังนี้

- มีความยาวอย่างน้อย 8-12 ตัวอักษรขึ้นไป
- มีทั้ง ตัวพิมพ์ใหญ่ + ตัวพิมพ์เล็ก
- มีตัวเลข และ สัญลักษณ์พิเศษ (เช่น @ , #)
- ไม่ใช่ข้อมูลส่วนตัว เช่น ชื่อ วันเกิด เบอร์โทร
- ไม่เป็นคำง่าย ๆ หรือคำที่เดาได้

ตัวอย่างรหัสผ่านที่ปลอดภัย อาทิ T9@kL2pZ7E และ Mx3Dp@ss2Q26

ตัวอย่างรหัสผ่านที่ไม่ปลอดภัย อาทิ 12345678 และ abc123

4. ความเป็นส่วนตัว (Privacy Management) การปกป้องข้อมูลส่วนบุคคล ไม่เปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน เลขบัตรประชาชน

5. มารยาททางดิจิทัล (Digital Etiquette) การสื่อสารอย่างสุภาพ เคารพผู้อื่น ไม่ใช้คำหยาบ หรือสร้างความขัดแย้ง

6. การรู้เท่าทันสื่อ (Media Literacy) สามารถวิเคราะห์ แยกแยะข่าวจริงข่าวปลอม และไม่แชร์ข้อมูลที่ไม่ถูกต้อง

Shareware คือ ซอฟแวร์ที่ให้ผู้ใช้งานทดลองใช้งานได้ฟรีในช่วงเวลาหนึ่ง หรือจำกัดฟีเจอร์บางส่วนหลังหมดช่วงทดลอง ต้องซื้อเพื่อใช้งานต่อ

7. การจัดการการกลั่นแกล้งทางไซเบอร์ หรือการสะกดรอยตามทางไซเบอร์ คือ การตามรังควานหรือเฝ้าติดตามคนอื่นทางออนไลน์อย่างไม่เหมาะสม รู้วิธีรับมือเมื่อถูกกลั่นแกล้ง เช่น บล็อก แจ้งรายงาน หรือขอความช่วยเหลือ ถ้าต้องการป้องกันการถูกติดตาม แนะนำใช้ร่วมกันหลายแบบ ใช้แอป DuckDuckGo/Firefox Focus บล็อกตัวติดตาม

8. ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) การตั้งรหัสผ่านที่ปลอดภัย อัปเดตซอฟต์แวร์ และระวังการเข้าถึงข้อมูล

ความสำคัญของความฉลาดทางดิจิทัล ช่วยให้ใช้งานเทคโนโลยีได้อย่างปลอดภัย ลดความเสี่ยงจากภัยคุกคามออนไลน์ ส่งเสริมการสื่อสารที่ดีในสังคมดิจิทัล ช่วยให้ตัดสินใจจากข้อมูลได้อย่างมีวิจารณญาณ เตรียมความพร้อมในการใช้ชีวิตและการทำงานในยุคดิจิทัล

แนวทางการพัฒนาความฉลาดทางดิจิทัล ฝึกคิดวิเคราะห์ก่อนเชื่อหรือแชร์ข้อมูล ตั้งค่าความเป็นส่วนตัวในโซเชียลมีเดีย ใช้รหัสผ่านที่ปลอดภัยและไม่ซ้ำกัน จำกัดเวลาใช้งานหน้าจอให้เหมาะสม เรียนรู้เทคโนโลยีใหม่อย่างต่อเนื่อง เคารพสิทธิและความคิดเห็นของผู้อื่น

ประโยชน์ที่ได้รับต่อตนเอง

1. ใช้เทคโนโลยีได้อย่างปลอดภัย
2. รู้เท่าทันภัยออนไลน์
3. ปกป้องข้อมูลส่วนตัวได้ดีขึ้น
4. เข้าใจการตั้งค่าความเป็นส่วนตัว และไม่เปิดเผยข้อมูลสำคัญโดยไม่จำเป็น
5. คิดวิเคราะห์ข้อมูลได้อย่างมีวิจารณญาณ แยกแยะข่าวจริงข่าวปลอม (Fake News) ได้
6. สื่อสารออนไลน์ได้อย่างเหมาะสม ใช้คำพูดสุภาพเคารพผู้อื่น
7. ลดปัญหาความขัดแย้ง
8. บริหารเวลาอยู่หน้าจอได้ดีขึ้น
9. ลดการติดมือถือหรือโซเชียล ใช้เวลาอย่างสมดุล

ประโยชน์ที่ได้รับต่อหน่วยงาน

1. บุคลากรสามารถใช้เทคโนโลยีได้อย่างถูกต้อง รวดเร็ว และลดความผิดพลาด
2. พนักงานมีความรู้ในการป้องกันภัยทำให้องค์กร ปลอดภัยมากขึ้น
3. การใช้งานสื่อดิจิทัลอย่างเหมาะสมช่วยให้หน่วยงาน ดูน่าเชื่อถือ
4. เสริมสร้างภาพลักษณ์ที่ดีขององค์กร
5. สามารถปรับตัวกับเทคโนโลยีใหม่ ๆ และการเปลี่ยนแปลงได้รวดเร็ว
6. ลดความเสียหายจากความผิดพลาด หรือภัยคุกคาม และใช้ทรัพยากรอย่างคุ้มค่า