

ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (understanding and using digital technology)

1. หลักจริยธรรมพื้นฐาน 4 ประการ (PAPA)

1. ความเป็นส่วนตัว (Privacy): เคารพสิทธิข้อมูลส่วนบุคคล ไม่สอดแนมหรือเปิดเผยข้อมูลของผู้อื่น
2. ความถูกต้อง (Accuracy): ไม่สร้างข้อมูลเท็จ ไม่บิดเบือนข้อมูล และตรวจสอบความน่าเชื่อถือของข้อมูลก่อนเผยแพร่
3. ความเป็นเจ้าของ (Property): ไม่คัดลอกโปรแกรม ผลงาน หรือละเมิดลิขสิทธิ์ทางปัญญาของผู้อื่น
4. การเข้าถึงข้อมูล (Accessibility): ไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์ที่ตนเองไม่มีสิทธิ์ และไม่รบกวนการทำงานของผู้อื่น

ข้อปฏิบัติ 10 ประการสำหรับผู้ใช้อินเทอร์เน็ต (โดยย่อ)

1. ต้องไม่ใช้อินเทอร์เน็ตทำร้าย/ละเมิดผู้อื่น
2. ต้องไม่รบกวนการทำงานของผู้อื่น
3. ต้องไม่สอดแนม/แอบดูเพิ่มข้อมูลผู้อื่น
4. ต้องไม่ใช้อินเทอร์เน็ตเพื่อการโจรกรรมข้อมูล
5. ต้องไม่ใช้อินเทอร์เน็ตสร้างหลักฐานที่เป็นเท็จ
6. ต้องไม่คัดลอกโปรแกรมที่มีลิขสิทธิ์
7. ต้องไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์
8. ต้องไม่นำผลงานผู้อื่นมาเป็นของตน
9. ต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคมที่เกิดจากการกระทำของท่าน
10. ต้องใช้อินเทอร์เน็ตโดยเคารพกฎระเบียบ กติกา และมีมารยาท

การกำหนดสิทธิการเข้าถึงข้อมูล (Access Control/Permission) คือการควบคุมความปลอดภัยโดยจำกัดสิทธิ์ผู้ใช้งาน (Viewer, Commenter, Editor) ในการเข้าถึง แก้ไข หรือแบ่งปันข้อมูลและระบบ เพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคลและข้อมูลสำคัญตามกฎหมาย PDPA โดยการจัดการทำได้ผ่านการตั้งค่าสิทธิ์ผู้ใช้งานแอปพลิเคชันหรือระบบจัดการข้อมูล (เช่น Google Drive, เอกสารองค์กร)

รายละเอียดการกำหนดสิทธิการเข้าถึง ระดับของสิทธิ (Permission Levels):

1. Viewer (ผู้ดู): ดูได้อย่างเดียว แก้ไขไม่ได้
2. Commenter (ผู้แสดงความคิดเห็น): สามารถดูและคอมเมนต์ได้ แต่แก้ไขเนื้อหาไม่ได้
3. Editor (ผู้แก้ไข): สามารถแก้ไข แก้ไขไฟล์ ได้เต็มรูปแบบ
4. Full Control/Owner: สิทธิ์สูงสุดในการจัดการ ตั้งค่า และจำกัดสิทธิ์ผู้อื่น

2. **Big Data** คือ ชุดข้อมูลขนาดใหญ่ ที่มีปริมาณมหาศาล หลากหลายรูปแบบ อาทิเช่น ฐานข้อมูลขององค์กร ฐานข้อมูลลูกค้า ข้อมูลโซเชียลมีเดีย ข้อมูลพฤติกรรมผู้บริโภค และอื่น ๆ ซึ่งต้องใช้เทคโนโลยีและซอฟต์แวร์เฉพาะทางในการเก็บรวบรวม จัดการ และวิเคราะห์

โดย Big Data จะมีทั้งข้อมูลที่มีโครงสร้าง กึ่งมีโครงสร้าง และไม่มีโครงสร้าง ขนาดของ Big Data ก็จะมีการเพิ่มขนาดของข้อมูลขึ้นไปเรื่อยๆ จากปัจจุบันที่มีขนาดข้อมูลหลายพัน Terabytes ก็จะมีการเพิ่มขนาดเป็น Zettabytes

ข้อมูลขนาดใหญ่ประกอบด้วยสามประเภทหลักได้แก่:

1. ข้อมูลที่มีโครงสร้างคือข้อมูลที่จัดระเบียบและง่ายต่อการสืบค้น เช่น แดวในฐานข้อมูลลูกค้า
2. ข้อมูลที่ไม่มีโครงสร้าง คือข้อมูลที่ไม่มีรูปแบบตายตัว และมักรวมถึง โพสต์ในโซเชียลมีเดีย ไฟล์วิดีโอและเสียง รูปภาพ หรืออีเมล
3. ข้อมูลกึ่งโครงสร้างคือข้อมูลที่อยู่ระหว่างข้อมูลสองประเภทก่อนหน้า และมักใช้รูปแบบเช่น JSON หรือ XML ซึ่งมีโครงสร้างอยู่บ้างแต่ไม่มีแบบแผนที่ตายตัว

ลักษณะสำคัญของ Big Data จะต้องมีลักษณะสำคัญ 4V ดังต่อไปนี้ จึงจะเรียกได้ว่าเป็น Big Data

1. ปริมาณ (Volume) คือ ปริมาณข้อมูลที่สามารถผลิตและจัดเก็บไว้ได้จะต้องขนาดที่ใหญ่มากเพียงพอ ซึ่งปริมาณของข้อมูลจะเป็นข้อบ่งบอกได้ถึงคุณภาพและประสิทธิภาพของข้อมูลภายในนั้น และสามารถนำไปพิจารณาต่อได้ว่าข้อมูลที่มีอยู่เหล่านั้น ถือเป็น Big Data หรือไม่

2. ความหลากหลาย (Variety) คือ ความหลากหลายของประเภทของข้อมูล โดยสามารถเพิ่มประสิทธิภาพในการนำข้อมูลไปวิเคราะห์ต่อยอดได้ ไม่ว่าจะเป็นข้อมูลที่เป็นตัวหนังสือ, รูปภาพ, ข้อมูลเสียงที่ถูกบันทึกไว้, วิดีโอหรือไฟล์ประเภทอื่นจากหลากหลายแหล่งที่มา ก็สามารถเป็นส่วนหนึ่งในการเพิ่มประสิทธิภาพการทำงานของ Big Data ได้ ซึ่งจะเป็นข้อมูลจากทุกฝ่ายไม่ว่าจะเป็นการเงิน ฝ่ายขาย การตลาด ลูกค้าสัมพันธ์ บัญชี รวมถึงตัวหนังสือที่อาจเป็นบทสนทนาระหว่างแผนก หรือระหว่างบริษัท ซึ่งอาจเป็นข้อความจาก Social Media รวมถึง URLs ที่มีข้อมูลเข้ามาอยู่ในทุกวัน

3. ความเร็ว (Velocity) คือ ความเร็วในการประมวลผลและผลิตข้อมูลขึ้นมาเพื่อให้ทันกับความต้องการของผู้ใช้งาน ซึ่ง Big Data คือข้อมูลที่ได้มาแบบ Real-Time และประมวลผลอยู่ตลอดเวลา แตกต่างจาก Small Data ที่ไม่สามารถทำได้ Big Data จะมีความถี่ในการประมวลผลที่มากกว่า การบันทึกข้อมูลที่มากกว่า และเผยแพร่ข้อมูลที่มากกว่า ข้อมูลของ Big Data ที่มีอัตราการเพิ่มขึ้นของข้อมูลที่มีการเพิ่มขึ้นได้อย่างรวดเร็ว โดยไม่ว่าจะเป็น ข้อมูลตัวอักษรการสนทนา ข้อมูลการบันทึกเสียง ข้อมูลการถ่ายภาพวิดีโอ ข้อมูลอัตราการสั่งซื้อสินค้า ข้อมูลโปรโมชันต่างๆ ซึ่งหากมานั่งดูแล้วจะถือว่าเป็นข้อมูลที่มีอยู่มาก และมีการอัปเดตเคลื่อนไหวยุ่ตลอดเวลา

4. คุณภาพของข้อมูล (Veracity) คือ คุณภาพของข้อมูลที่สามารถนำไปวิเคราะห์ข้อมูลต่อไปได้อีก เป็นข้อมูลที่ยังไม่ผ่านการประมวลผลอยู่ในรูปแบบของข้อมูลดิบซึ่งสามารถนำไปประมวลผลต่อไปได้ และเป็นข้อมูลที่มาจากหลากหลายแหล่งไม่ว่าจะเป็น Facebook, Youtube, Twitter ซึ่งข้อมูลจากแหล่งเหล่านี้ยากที่จะสามารถควบคุมคุณภาพรวมถึงการคัดกรองข้อมูล และความน่าเชื่อถือของข้อมูล จึงต้องนำข้อมูลเหล่านี้ เข้าสู่กระบวนการทำ Data Cleansing

3. ความปลอดภัยยุคดิจิทัล (Digital Safety & Security) คือความรู้ ทักษะ และการปฏิบัติเพื่อปกป้องข้อมูลส่วนบุคคล อุปกรณ์ และเครือข่ายจากการโจมตีทางไซเบอร์ การฉ้อโกง และการกลั่นแกล้งออนไลน์ โดยเน้นการสร้างความรู้ตระหนักรู้เท่าทันภัย เช่น มัลแวร์, ฟิชซิง (Phishing) และการแอบอ้างตัวตน เพื่อใช้งานอินเทอร์เน็ตได้อย่างมั่นใจและยั่งยืน

แนวทางปฏิบัติเพื่อความปลอดภัยในยุคดิจิทัล

1. สร้างรหัสผ่านที่ปลอดภัย: ใช้รหัสผ่านที่ซับซ้อน ไม่ซ้ำกันในแต่ละบัญชี และเปิดการยืนยันตัวตนแบบสองชั้น (2FA)
2. อัปเดตซอฟต์แวร์เสมอ: ปรับปรุงระบบปฏิบัติการและแอปพลิเคชันให้เป็นเวอร์ชันล่าสุดเพื่อปิดช่องโหว่ความปลอดภัย
3. ตั้งค่าความเป็นส่วนตัว: ตรวจสอบและจำกัดการเข้าถึงข้อมูลส่วนบุคคลในโซเชียลมีเดีย
4. ระวังภัยคุกคามออนไลน์: ไม่คลิกลิงก์หรือดาวน์โหลดไฟล์จากอีเมล/ข้อความที่ไม่รู้จัก
5. สำรองข้อมูลสำคัญ: ทำการสำรองข้อมูล (Backup) ไว้เป็นประจำเพื่อป้องกันการสูญหายจากการถูกรื้อค่าได้
6. ใช้เครื่องมือป้องกัน: ติดตั้ง โปรแกรมแอนตี้ไวรัส (Anti-Virus) และไฟร์วอลล์ (Firewall) ที่เชื่อถือได้

ภัยคุกคามหลักในยุคดิจิทัล

- การฉ้อโกงทางการเงิน: การหลอกลวงผ่านแอปฯ หรือเว็บปลอม
 - มัลแวร์และแรนซัมแวร์: ไวรัสที่ขโมยข้อมูลหรือล็อกไฟล์เรียกค่าไถ่
 - การกลั่นแกล้งออนไลน์ (Cyber Bullying): การคุกคาม การประจาน หรือสร้างข่าวปลอม
- การตระหนักรู้ถึง รอยเท้าดิจิทัล (Digital Footprint) และการจัดการข้อมูลอย่างรอบคอบเป็นหัวใจสำคัญของการรักษาความปลอดภัยในยุคปัจจุบัน

การเล่น social network ให้ปลอดภัย

1. คิดให้รอบคอบ ก่อน โพสต์คลิกก่อน
2. ระวังคลิก link
3. พิมพ์ URL โดยตรง
4. รอบคอบก่อนรับใครเป็นเพื่อน
5. ตั้งค่าความเป็นส่วนตัว
6. ไม่แสดงข้อมูลส่วนตัว เช่น บัตรประชาชน
7. เปิดใช้งาน Do not track
8. ใช้วิจารณญาณก่อนตัดสินใจ อย่าเชื่อทันที
9. ควบคุมการใช้งาน
10. สังคมเสรี/ทุกคนมีสิทธิ์แสดงความคิดเห็น

ข้อเท็จจริงและความคิดเห็น

ข้อเท็จจริงคือเหตุการณ์หรือข้อมูลจริงที่ตรวจสอบได้ มีความสมเหตุสมผล ส่วนข้อคิดเห็น คือ ความรู้สึก ความเชื่อ หรือทัศนคติส่วนตัวที่สอดแทรกอยู่ การแยกแยะทั้งสองส่วนออกจากกันช่วยให้รับข้อมูลได้อย่างมีวิจารณญาณ โดยข้อเท็จจริงมักมีหลักฐานเชิงประจักษ์ยืนยัน ส่วนข้อคิดเห็นมักจะมีคำว่า น่าจะ, อาจจะ, ควร, หรือเป็นความรู้สึกของผู้พูด

ลักษณะของข้อเท็จจริง (Fact)

- เป็นจริงและสมจริง: สามารถพิสูจน์ได้ว่าจริงหรือเท็จ
- มีหลักฐานอ้างอิง: มีข้อมูลที่เชื่อถือได้มารองรับ
- มีความสมเหตุสมผล: เป็นเหตุการณ์ที่เกิดขึ้นจริง
- ตัวอย่าง:

ลักษณะของข้อคิดเห็น (Opinion)

- แสดงความรู้สึก/ความเชื่อ: เป็นทัศนคติส่วนตัว
- แสดงการคาดคะเน: มักใช้คำว่า "น่าจะ", "อาจจะ"
- แสดงข้อเสนอแนะ: มักใช้คำว่า "ควร", "น่าจะ"

ปัจจุบันการแยกแยะเรื่องนี้มีความสำคัญมาก โดยเฉพาะการอ่านข่าวหรือโฆษณา เพื่อหลีกเลี่ยงการหลงเชื่อข้อมูลที่อาจคลาดเคลื่อน ทำให้เราสามารถใช้เวลาในโซเชียลมีเดียได้อย่างปลอดภัยและมีประสิทธิภาพ

ประโยชน์ที่ได้จากการศึกษาในบทเรียนนี้ แบ่งออกเป็น 2 ส่วน คือ

1. ประโยชน์ต่อตนเองคือ มีความรู้ความเข้าใจด้านสารสนเทศ สื่อ และเทคโนโลยีด้านดิจิทัลมากขึ้น
2. ประโยชน์ต่อหน่วยงาน คือ สามารถวิเคราะห์ แยกแยะ รู้เท่าทันสื่อดิจิทัล เพื่อเลือกนำไปใช้งานได้อย่างเหมาะสม มีความเข้าใจและปฏิบัติงานด้านดิจิทัลได้อย่างถูกต้องและปลอดภัย ตลอดจนตระหนักถึงภัยคุกคามด้านดิจิทัลและสามารถตรวจสอบการทำงานตามหลักการปฏิบัติงานที่ดีได้ในเบื้องต้น มีความรู้ในการใช้สื่อเพื่อผลิตข้อมูลในการถ่ายทอดองค์ความรู้เกี่ยวกับการพัฒนาที่ดิน เพื่อให้บริการด้านความรู้และเทคโนโลยีแก่เกษตรกรในพื้นที่โครงการหลวง



ผู้สรุปรายงาน นางสาวสุภาวดี บุญธรรม
นักวิชาการเกษตร ชำนาญการพิเศษ