

สรุปบทเรียนการพัฒนาความรู้

หลักสูตร

Digital Code of Merit

ชื่อ-สกุล นางสาวกรรภัทร นพมาลัย

ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ

สังกัด กลุ่มวิจัยและพัฒนาหมอดินอาสาและบริหารจัดการเครือข่าย กองวิจัยและพัฒนาการจัดการที่ดิน

วันที่อบรม 15-19 สิงหาคม 2569

วิทยากร ดร.สมิทธิ ดารากร ณ อยุธยา อาจารย์ประจำกลุ่ม

สาขาเทคโนโลยีการจัดการระบบสารสนเทศ คณะวิศวกรรมศาสตร์

มหาวิทยาลัยมหิดล

วัตถุประสงค์ของหลักสูตร

เพื่อให้ผู้เรียนมีความรู้ ความเข้าใจเกี่ยวกับจริยธรรมในการใช้เทคโนโลยี การเข้าถึงข้อมูล Data Accessibility ความเข้าใจเกี่ยวกับพระราชบัญญัติ ตลอดจนแนวทางปฏิบัติและมารยาทในสังคมดิจิทัล

สรุปบทเรียน

“Digital Code of Merit” เป็นแนวทางการใช้เทคโนโลยีดิจิทัลอย่างมีคุณธรรมและความรับผิดชอบ โดยเน้นการเคารพสิทธิของผู้อื่น การใช้เทคโนโลยีอย่างสร้างสรรค์ ปลอดภัย และมีมารยาทในสังคมดิจิทัล

หลักจริยธรรมในการใช้เทคโนโลยีคอมพิวเตอร์และสารสนเทศ (PAPA)

- 1) Privacy (ความเป็นส่วนตัว) ควบคุมข้อมูลของตนเองและเปิดเผยเฉพาะข้อมูลที่ได้รับอนุญาต
- 2) Accuracy (ความถูกต้อง) ตรวจสอบข้อมูลก่อนเผยแพร่ เพื่อให้ข้อมูลมีความน่าเชื่อถือ
- 3) Property (ความเป็นเจ้าของ) เคารพลิขสิทธิ์ สิทธิบัตร และทรัพย์สินทางปัญญา
- 4) Accessibility (การเข้าถึงข้อมูล) กำหนดสิทธิ์การเข้าถึงข้อมูลตามระดับผู้ใช้งาน เพื่อความปลอดภัย และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

มารยาทในการใช้อินเทอร์เน็ต 10 ข้อ (Netiquette) คือ จรรยาบรรณของการอยู่ร่วมกันในสังคมอินเทอร์เน็ตซึ่งไม่ต่างจากสังคมบนโลกแห่งความเป็นจริงที่จำเป็นต้องมีกฎกติกาสำหรับกำกับดูแลพฤติกรรมและปฏิสัมพันธ์ของสมาชิก ในการใช้งานสื่อสังคมออนไลน์ แต่ทุกคนควรจะคำนึงถึงมารยาทดังต่อไปนี้ 1. อย่าลืมนำกำลังสื่อสารอยู่กับมนุษย์จริง ๆ 2. ยึดมาตรฐานเดียวกับการสื่อสารในชีวิตจริง 3. รู้ว่าคุณอยู่ที่ไหนในไซเบอร์สเปซ 4. เคารพเวลาและการใช้แบนด์วิธ เมื่อไม่ใช้งานก็ควรออกจากระบบเพื่อเปิดโอกาสให้คนอื่นใช้งาน 5. แบ่งปันความรู้ที่ตนเองเชี่ยวชาญ 6. ช่วยกันควบคุมสงครามการใช้อารมณ์ รู้จักอดกลั้น ไม่โต้ตอบด้วยอารมณ์ 7. เคารพสิทธิส่วนบุคคลของผู้อื่น 8. อย่าใช้อำนาจในทางที่ผิด 10. รู้จักให้อภัยความผิดพลาดของผู้อื่น

การเอาใจใส่ผู้อื่น (Empathy) เป็นการปรับทัศนคติที่ดีเกี่ยวกับการรับรู้และเข้าใจพฤติกรรมที่แสดงออกในโลกอินเทอร์เน็ตของผู้อื่น และส่งเสริมจริยธรรมที่ดีงามเหมาะสมกับบริบทของสังคมและวัฒนธรรมไทย โดย 7 นิสัยที่ไม่ควรทำในกลุ่มไลน์ 1. อ่านแล้วไม่ตอบ 2. ส่งข้อความเร็ว ๆ ก่อกวนผู้อื่น 3. นำความลับของคนอื่นไป

เปิดเผย 4. พุดคุยเรื่องทีคนอื่นไม่รู้เรื่อง 5. แชร์ข่าวลือที่ไม่มีการตรวจสอบข้อเท็จจริง 6. ออกจากกลุ่มโดยไม่แจ้งเหตุผล

10 พฤติกรรมของคนติชโซเซียลเน็ตเวิร์ค การใช้โซเชียลเน็ตเวิร์คมากเกินไปก่อให้เกิดผลเสียหลายอย่างทั้งที่เกิดกับสุขภาพทางกาย ความสัมพันธ์กับผู้คนในสังคมของโลกแห่งความจริง สามารถประเมินตนเองว่ากำลังมีอาการติชโซเซียลเน็ตเวิร์ค ดังนี้ 1. ใส่ใจโทรศัพท์ทุกครั้งที่ได้ยินเสียงเตือน 2. กดไลค์ทุกเรื่อง 3. แชร์ทุกอย่างที่แชร์ได้ 4. เช็คอินทุกอย่างก้าว 5. เช็คความเคลื่อนไหวในโลกโซเซียลเน็ตเวิร์คตลอดเวลา 6. ไม่เป็นอันทำอะไรหลังโพสต์ข้อความบนโซเซียลเน็ตเวิร์ค 7. โพสต์คำคมตลอดเวลา 8. โพสต์ภาพอาหารทุกมือ 9. เล่นเกมบนโซเซียลเน็ตเวิร์คตลอดเวลาที่ว่าง 10. ใช้โซเซียลเน็ตเวิร์คแทนโทรศัพท์และช่องทางสื่อสารอื่น ๆ



การกลั่นแกล้งทางไซเบอร์ (Cyber Bullying) คือ การประทุษร้ายหรือทำให้ผู้อื่นอับอายผ่านการใช้อิเล็กทรอนิกส์ เพื่อแสดงความเป็นศัตรูหรือแสดงออกในแง่ลบต่ออีกฝ่าย พฤติกรรม Cyber Bullying ที่พบบ่อยคือ ให้อายด้วยถ้อยคำหยาบคาย แบล็คเมล คุกคามทางเพศออนไลน์ หลอกลวง แอบอ้างตัวตนของคนอื่น สร้างกลุ่มใน Social Network เพื่อโจมตีโดยเฉพาะ หากเจอการกลั่นแกล้งทางไซเบอร์ ดำเนินการได้ ดังนี้ (1) บอกให้หยุดอย่างหนักแน่นและชัดเจน (2) ถ้ารู้ว่าผู้ทำอยู่ที่ไหน อาจส่งจดหมายเตือนไปถึงบ้าน (3) รายงานพฤติกรรมต่อตำรวจ (5) รายงานไปยังหน่วยงานที่ดูแลความเรียบร้อยของโลกออนไลน์หรือบริษัทที่ให้บริการ บันทึกข้อความเก็บไว้เป็นหลักฐาน และ (6) บล็อกไม่ให้รับข้อความจากคนนั้น

การเผยแพร่ข้อมูลบนโลกออนไลน์ การเผยแพร่ข้อมูลส่วนตัว ไม่ว่าจะเป็นกิจกรรมที่ทำหรือสถานที่อยู่ อาจจะมีผู้ไม่หวังดีเก็บข้อมูลเหล่านี้ อาจจะทำร้ายผู้โพสต์ภายหลังได้ โดยหากเป็นพฤติกรรมที่ไม่เหมาะสมเจ้าหน้าที่สามารถติดตามมาปรับได้ เนื่องจากข้อมูลที่ถูกแชร์บนโลกไซเบอร์จะสามารถย้อนกลับไปได้หาผู้แชร์ได้เสมอ ดังนั้นผู้ใช้งานต้องระมัดระวัง ในการแชร์ข้อมูลต่าง ๆ ไม่ควรแชร์ข้อมูลส่วนตัว ข้อมูลไม่เหมาะสม หรือข้อมูลที่ไม่แน่ใจว่าเป็นความจริง เมื่อเห็นข้อมูลใด ๆ ก่อนตัดสินใจส่งต่อข้อมูลให้พิจารณาข้อมูลในปัจจัยต่าง ๆ ดังนี้ **Who** ใครเป็นผู้แชร์ข้อมูล สามารถเชื่อถือได้แค่ไหน **What** เป็นเรื่องที่ถูกต้องหรือไม่ **When/Where** กาลเทศะและความทันสมัยของข้อมูล **Why** ในการเผยแพร่ข้อมูลนั้นใครคือผู้ได้ประโยชน์ **How** วิธีการเผยแพร่ข้อมูลเป็นอย่างไร ยิ่งเป็นวิธีที่เน้นกระตุ้นความรู้สึกยิ่งน่าสงสัย

การรักษาความเป็นส่วนตัว (Privacy) เพื่อป้องกันมิให้ผู้อื่นเข้าถึงข้อมูลส่วนตัว ควรปฏิบัติดังนี้ สังเกตก่อนคลิก ไม่ว่าจะเป็นเว็บไซต์ วิดีโอ รูปภาพ เพื่อให้แน่ใจว่าไม่ได้ลิงค์ต่อไปยังเพจที่ไม่ปลอดภัย ใช้การพิมพ์ URL แทนการคลิกลิงค์ที่ถูกส่งมา ไม่ควรตั้งรหัสผ่านที่เดาได้ง่าย เช่น 123456 qwerty วันเดือนปีเกิด ไม่ตั้งชื่อผู้ใช้และรหัสผ่านเหมือนกันทุกบัญชี ออกจากระบบทุกครั้งหลังเลิกใช้งาน ติดตั้งระบบป้องกันไวรัสและ Update สม่าเสมอ

การตั้งรหัสผ่าน โดยรหัสผ่านที่ไม่ควรใช้ ใช้รหัสผ่านเดียวกันกับทุกโปรแกรม รหัสผ่านที่คาดเดาง่าย เช่น 123456 qwerty ใช้ข้อมูลบุคคลเป็นรหัสผ่าน เช่น วันเดือนปีเกิด หมายเลขโทรศัพท์ ใช้คำที่มีความหมายในพจนานุกรม ใช้เฉพาะตัวอักษรอย่างเดียว ใช้รหัสผ่านเดิมไม่เคยเปลี่ยนเลย **รหัสผ่านที่ดี** ควรมีความยาวอย่างน้อย 7 ตัวอักษร ประกอบด้วยอักษรตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข สัญลักษณ์พิเศษ ใช้สัญลักษณ์อย่างน้อย 1 ตัว

การถอดรหัสผ่าน โดยมีผู้ทำการวิจัยและประมาณระยะเวลาที่จะต้องใช้ในการถอดรหัสผ่านไว้ดังนี้ หากตั้งรหัสผ่านความยาว 6 ตัวอักษร ใช้เฉพาะอักษรตัวพิมพ์เล็ก เช่น darren ใช้เวลาถอดรหัส ประมาณ 5 นาที หากตั้งรหัสผ่านความยาว 7 ตัวอักษรโดยใช้อักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ และตัวเลข เช่น Land3rz ใช้เวลาถอดรหัสประมาณ 1 เดือนครึ่ง หากตั้งรหัสผ่านความยาว 8 ตัวอักษรโดยใช้อักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ เช่น B33r&sdA ใช้เวลาถอดรหัสประมาณ 229 ปี

เวลาที่ใช้ในการถอดรหัสผ่าน		
5 นาที	เดือนครึ่ง	229 ปี
		
รหัสผ่านมีความยาว 6 ตัว มีตัวอักษรเล็กอย่างเดียว เช่น darren	รหัสผ่านมีความยาว 7 ตัว มีตัวอักษรเล็กใหญ่และตัวเลข เช่น Land3rz	รหัสผ่านมีความยาว 8 ตัว มีตัวอักษรเล็กใหญ่และตัวเลข และอักขระพิเศษ เช่น B33r&sdA
หมายเหตุ: เวลาในการถอดรหัสอยู่ที่ 1,000,000 ชุดต่อวินาที 		



อันตรายบนโลกอินเทอร์เน็ต (Dangerous Online) 6 ข้อควรระวังในการใช้งานอินเทอร์เน็ต ดังนี้ (1) ไม่บอกข้อมูลส่วนตัว (2) หากพบภาพหรือข้อความไม่เหมาะสมให้แจ้งผู้ปกครอง (3) ไม่ควรไปพบบุคคลที่รู้จักบนอินเทอร์เน็ต (4) ไม่ส่งรูปหรือข้อมูลของตัวเองให้กับคนที่รู้จักบนอินเทอร์เน็ต (5) ไม่ตอบคำถามหรือสื่อข้อความหยาบคาย (6) เคารพข้อตกลงในการใช้งาน

กฎหมายคุ้มครองการกระทำผิดคอมพิวเตอร์ เช่น มาตรา 12 แห่ง พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 กำหนดบทลงโทษที่รุนแรงขึ้น สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่พุ่งเป้าไปที่ระบบสำคัญของประเทศ เช่น ความมั่นคง ปลอดภัย ความปลอดภัยสาธารณะ เศรษฐกิจ หรือโครงสร้างพื้นฐาน ทั้งนี้มีหน่วยงานที่เกี่ยวข้อง คือ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สังกัดกองบัญชาการตำรวจสอบสวนกลาง (CIB) มีหน้าที่หลักในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี คดีคอมพิวเตอร์ และภัยไซเบอร์ต่างๆ

Cyber Stalking คือ การส่องหรือแอบติดตามชีวิตและการเคลื่อนไหวของบุคคลใดบุคคลหนึ่งบนโลก Social โดยไม่ให้อีกฝ่ายรู้ พฤติกรรมลักษณะนี้เป็นการสะท้อนปัญหาทางสุขภาพจิตและอาจผิดกฎหมาย โดยนักจิตวิทยาระบุว่า Cyber Stalking แตกต่างจากการค้นหาข้อมูลของคนที่เราสนใจตรงที่ Cyber Stalking เป็นพฤติกรรมที่ทำต่อเนื่องกันอย่างไม่ลดละ และผู้ตกเป็นเป้ารู้สึกกลัว บางคนเมื่อติดตามแล้วมีพฤติกรรมเลียนแบบบุคคลที่เป็นเป้าหมาย พยายามใช้ชีวิตแบบเดียวกับเป้าหมายอาจก่อให้เกิดปัญหากับตนเอง เช่น ชื่อของราคาแพงเลียนแบบดารานักแสดงมีปัญหาทางการเงิน

ประโยชน์ที่ได้รับต่อตนเอง หลักสูตรดังกล่าวช่วยเสริมสร้างทักษะและความรู้ในการป้องกันตนเองจากภัยออนไลน์ โดยสามารถรู้เท่าทันกลลวงและข้อมูลเท็จ (Fake News) ตลอดจนลดความเสี่ยงในการตกเป็นเหยื่อหรือเป็นผู้ส่งต่อข้อมูลที่ไม่ถูกต้อง นอกจากนี้ ยังช่วยยกระดับมารยาทและทักษะการสื่อสารในโลกดิจิทัล ทำให้ตระหนักถึงความสำคัญของการใช้วิจารณญาณก่อนเผยแพร่หรือแบ่งปันข้อมูลบนสื่อสังคมออนไลน์ รวมถึงการเคารพสิทธิและความเป็นส่วนตัวของผู้อื่น โดยยึดหลักว่า “การสื่อสารในโลกดิจิทัลเป็นไปอย่างรวดเร็ว จึงต้องใช้วิจารณญาณและยึดมั่นในจริยธรรมก่อนเผยแพร่ข้อมูลเสมอ”

ประโยชน์ที่ได้รับต่อหน่วยงาน (1) ลดความเสี่ยงจากพฤติกรรมของบุคลากรที่อาจส่งผลกระทบต่อภาพลักษณ์องค์กรบนโลกออนไลน์ (2) ยกระดับมาตรฐานความปลอดภัยไซเบอร์ภายในองค์กร จากการจัดการข้อมูลที่ถูกต้องตามหลักจริยธรรม (3) ส่งเสริมสภาพแวดล้อมการทำงานที่เคารพสิทธิ ความเป็นส่วนตัว และความเท่าเทียมในการเข้าถึงข้อมูล