

หลักสูตร Digital Code of Merit

(แนวปฏิบัติและมารยาทในสังคมดิจิทัล)

โดย นางสาวพรพรรณ แสนบุญศิริ
นักวิชาการแผนกที่ภาพถ่ายชำนาญการ

วัตถุประสงค์

- เพื่อเรียนรู้ความหมายของจริยธรรมในการใช้เทคโนโลยีสารสนเทศ
- เพื่อเรียนรู้การเข้าถึงข้อมูล Data Accessibility
- เพื่อเรียนรู้เกี่ยวกับแนวปฏิบัติในสังคมดิจิทัล (Digital Etiquette)

๑. มารยาทในการใช้เทคโนโลยีสารสนเทศ

จริยธรรม หมายถึง หลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็นแนวทางในการปฏิบัติหรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศโดยยึดหลักความถูกต้องเป็นเกณฑ์ในการปฏิบัติร่วมกัน ๔ ประเด็นคือ

๑.๑ ความเป็นส่วนตัว (Privacy) คือ สิทธิของแต่ละบุคคลในการตัดสินใจว่าข้อมูลข่าวสารของตนจะเปิดเผยต่อบุคคลอื่นเมื่อใด อย่างไร และมีขอบเขตมากน้อยเพียงใด

๑.๒ ความถูกต้อง (Accuracy) คือ การตรวจสอบความถูกต้องของข้อมูลก่อนเปิดเผยเสมอ

๑.๓ ความเป็นเจ้าของ (Property) คือ กรรมสิทธิ์ในการถือครองทรัพย์สินทั้งจับต้องได้และจับต้องไม่ได้

๑.๔ การเข้าถึงข้อมูล (Data accessibility) คือ การรักษาความปลอดภัยและการเข้าถึงความลับของข้อมูล

มารยาทการใช้อินเทอร์เน็ต มีกฎกติกา มารยาทที่เป็นมาตรฐาน ๑๐ ข้อดังนี้

- การสื่อสารด้วยภาษาที่เหมาะสม
- ปฏิบัติตามกฎระเบียบจรรยาที่พึงปฏิบัติทั้งในสังคมโลกและในสังคมอินเทอร์เน็ต
- รู้ว่าคุณอยู่ที่ไหนในไซเบอร์สเปซ
- เคารพเวลาและการใช้แบนด์วิธ เพื่อเปิดโอกาสให้ผู้อื่นได้ใช้เครือข่าย
- ทำตัวเองให้ดูดีเสมอเมื่ออยู่ในโลกออนไลน์
- แบ่งปันความรู้ที่ตนเองเชี่ยวชาญ
- ช่วยกันควบคุมสงครามการใช้อารมณ์
- เคารพสิทธิส่วนบุคคลของผู้อื่น
- อย่าใช้อำนาจในทางที่ผิด
- รู้จักให้อภัยกับความผิดพลาดของผู้อื่น

๒. การเอาใจใส่ผู้อื่น (Empathy) คือ การปรับทัศนคติที่ดีเกี่ยวกับการรับรู้และเข้าใจพฤติกรรมที่แสดงออกในโลกอินเทอร์เน็ตของผู้อื่น และส่งเสริมจริยธรรมที่ดีงามเหมาะสมกับบริบทของสังคมและวัฒนธรรมไทย

๓. การกลั่นแกล้งทางไซเบอร์ (Cyber Bullying) คือ การประทุษร้ายหรือทำให้ผู้อื่นอับอายผ่านทางการใช้สื่ออิเล็กทรอนิกส์ เพื่อแสดงความเป็นศัตรูหรือแสดงออกในแง่ลบต่ออีกฝ่ายจึงมีแนวทางปฏิบัติเพื่อไม่ให้เกิดการรังแกในโลกไซเบอร์ดังนี้

- บอกนักเลงคนนั้นอย่างชัดเจนและหนักแน่นให้หยุดพฤติกรรมเสียที
- ถ้านักเลงเป็นคนที่รู้จักเช่นเพื่อนของลูกอาจแจ้งกับอาจารย์ที่โรงเรียนให้ช่วยเหลือด้วย
- รายงานพฤติกรรมมารังแกต่อเจ้าหน้าที่ตำรวจ
- รายงานไปยังหน่วยงานที่ดูแลความเรียบร้อยของโลกออนไลน์หรือบริษัทให้บริการ

๓.๕ บันทึกข้อความที่เป็นการรังแกเก็บไว้เพื่อเป็นหลักฐาน

๓.๖ บล็อก/ไม่รับข้อความจากคนนั้น

๔. การเผยแพร่ข้อมูลบนโลกออนไลน์ (Sharing Society)

สื่อสังคมออนไลน์ที่เผยแพร่ข้อมูลในรูปแบบต่างๆทำให้สามารถโต้ตอบกันระหว่างผู้ส่งสารกับผู้รับสารสังคมในโลกออนไลน์ได้ซึ่งจะมีทั้งคนดีและคนไม่ดีปะปนกันไปรวมถึงการแพร่กระจายข้อมูลได้ในเวลาอันรวดเร็วดังนั้นการใช้สื่อสังคมออนไลน์จึงมีข้อควรปฏิบัติและข้อควรระวังในการใช้ เช่น

๔.๑ ผู้เผยแพร่/ผู้โพสต์ข้อความหรือแสดงความคิดเห็นซึ่งเป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะบนสื่อสังคมออนไลน์ต้องรับผิดชอบทั้งด้านสังคมและกฎหมาย

๔.๒ ไม่ควรเปิดเผยข้อมูลส่วนตัวรวมถึงข้อมูลทางการเงินบนสื่อสังคมออนไลน์

๔.๓ ไม่ควรโพสต์หรือส่งต่อข้อมูลรูปภาพวิดีโอที่ทำให้ผู้อื่นเสียหาย เช่น ภาพหลุด คลิปหลุด รวมถึงการใช้ถ้อยคำหยาบคายให้ร้ายผู้อื่นในทางเสียหายหรือสร้างความแตกแยกในสังคม

๔.๔ ไม่ควรเชื่อใจคนอื่นในการแลกเปลี่ยนข้อมูลส่วนตัวผ่านอินเทอร์เน็ต เช่น อีเมล หมายเลขโทรศัพท์ที่อยู่ อาจถูกหลอกลวงไปทำอันตรายได้

๔.๕ ควรระมัดระวังในการเช็คอิน (Check-in) ผ่านสื่อสังคมออนไลน์

ในขณะที่ใช้งานอินเทอร์เน็ต ก่อนตัดสินใจส่งต่อข้อมูลใดๆ ควรพิจารณาปัจจัยต่างๆ ดังนี้

๑. ใครเป็นผู้แชร์ข้อมูล
๒. ข้อมูลนั้นๆ เป็นเรื่องที่ถูกต้องหรือไม่
๓. กาลเทศะและความทันสมัยของข้อมูล
๔. การเผยแพร่ข้อมูลนั้นใครคือผู้ได้ประโยชน์
๕. วิธีการเผยแพร่ข้อมูลเป็นอย่างไร

๕. การระมัดระวังอันตรายบนโลกอินเทอร์เน็ต (Dangerous online)

การรู้จักระมัดระวังและป้องกันเหตุการณ์ที่อาจเกิดขึ้นในยุคดิจิทัลหรืออันตรายที่แฝงอยู่ในการใช้อินเทอร์เน็ตในปัจจุบันซึ่งมี ๖ ข้อที่ควรระวังในการใช้งานอินเทอร์เน็ต ดังนี้

- ๕.๑ ไม่บอกข้อมูลส่วนตัวเช่นที่อยู่เบอร์โทรศัพท์
- ๕.๒ กล่าวตักเตือนเยาวชนหากพบข้อความหรือรูปภาพใดๆ หรือแจ้งผู้ปกครองของเยาวชน
- ๕.๓ ไม่พบบุคคลใดๆ ที่รู้จักทางอินเทอร์เน็ต
- ๕.๔ ไม่ส่งรูปหรือหรือสิ่งใดๆ ให้บุคคลที่ไม่รู้จัก
- ๕.๕ ไม่ตอบคำถามหรือสื่อสารด้วยข้อความที่หยาบคาย
- ๕.๖ เคารพต่อข้อตกลงในการใช้อินเทอร์เน็ต

๖. **ไซเบอร์สต็อกกิ้ง (Cyber Stalking)** คือ การส่องหรือแอบติดตามชีวิตและการเคลื่อนไหวของบุคคลใดบุคคลหนึ่งบนโลกไซเบอร์โดยที่ไม่ให้อีกฝ่ายรู้ ซึ่งสะท้อนถึงปัญหาสุขภาพจิตอีกทั้งยังอาจผิดกฎหมายด้วย

นักจิตวิทยาระบุว่า Cyber Stalking หรือการเกาะติดชีวิตออนไลน์ของผู้อื่น แตกต่างจากการค้นหาข้อมูลของคนที่เราสนใจตรงที่ Cyber Stalking เป็นพฤติกรรมที่ทำต่อเนื่องอย่างไม่ลดละ และผู้ที่ตกเป็นเป้ารู้สึกกลัวได้พฤติกรรมหมกมุ่นติดตามคนบนอินเทอร์เน็ตเป็นผลมาจากสุขภาพจิตที่มีปัญหาอยู่แล้ว อาจพบในผู้ที่มีการซึมเศร้า ชี้อ่อนแอและตีตัวออกห่างจากสังคม

แนวปฏิบัติหากถูกคุกคามจาก Cyber Stalking ควรดำเนินการดังนี้

๑. ตั้งสติและรวบรวมหลักฐานให้มากที่สุด เช่น ภาพถ่ายที่ถูกแบล็กเมล์ แชทข้อความ ข้อมูลคนร้าย ฯลฯ
๒. เปลี่ยนอีเมลและรหัสผ่านบัญชีออนไลน์ทั้งหมด
๓. แจ้ง Help Center ของผู้ให้บริการที่เกี่ยวข้อง เช่น Facebook
๔. อย่าตอบโต้หรือนัดพบกับ Cyber Stalker เด็ดขาด
๕. ติดต่อสถานีตำรวจท้องที่เกิดเหตุทันทีหรือร้องทุกข์ที่กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

พฤติกรรม Cyber Stalking ในประเทศไทยยังไม่มีกฎหมายที่เอาผิด Cyber Stalker เหมือนบางประเทศในแถบตะวันตก หากพฤติกรรมนี้เป็นเพียงการแอบส่องดูเฉย ๆ ไม่เกิดความเสียหายชัดเจน แต่ถ้ามีการพัฒนาขึ้นเป็นการคุกคามทำให้เหยื่อรู้สึกเดือดร้อน รำคาญ หรือรู้สึกไม่ปลอดภัย อาจเข้าข่ายฐานความผิดตามประมวลกฎหมายอาญา มาตรา ๓๙๗ ผู้ใดกระทำความผิดด้วยประการใด ๆ ต่อผู้อื่นอันเป็นการรังแกข่มเหง คุกคาม หรือกระทำให้ได้รับความอับอายหรือเดือดร้อนรำคาญ ต้องระวางโทษปรับไม่เกินห้าพันบาท หรือในกรณีที่มีการลอบเข้าระบบคอมพิวเตอร์ของเหยื่อด้วยจะเข้าข่ายความผิดตาม พรบ. คอมพิวเตอร์ ๒๕๖๐ มาตรา ๕ ถึง มาตรา ๘ ว่าด้วยการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลฯ ของผู้อื่นโดยไม่ชอบต้องระวางโทษจำคุกสูงสุด ๒ ปี และ/หรือปรับสูงสุด ๔ หมื่นบาท

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

๑. ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตให้เป็นเวอร์ชันใหม่อย่างสม่ำเสมอ ตรวจสอบไฟล์แนบทางอีเมลและระมัดระวังก่อนจะกดคลิกลิงก์เชื่อมโยงไปยังส่วนอื่นๆ
๒. สำรองข้อมูลไว้เพื่อป้องกันข้อมูลสูญหาย
๓. การเข้ารหัสป้องกันการเข้าถึงข้อมูลที่อยู่ในอุปกรณ์เชื่อมต่อภายนอก

ประโยชน์ที่ได้รับ

๑. มีความรู้ความเข้าใจเกี่ยวกับจริยธรรมในการใช้เทคโนโลยีสารสนเทศในโลกดิจิทัล
๒. ปฏิบัติตนในการใช้เทคโนโลยีสารสนเทศในโลกดิจิทัลในการปฏิบัติงานและการใช้ชีวิตประจำวันได้อย่างมีมารยาท ทั้งมารยาทการใช้งานอินเทอร์เน็ตและมารยาทการใช้โทรศัพท์ในที่สาธารณะ รวมทั้งการระมัดระวังไม่ให้เกิดการกลั่นแกล้งในโลกไซเบอร์
๓. มีความรู้ความเข้าใจเกี่ยวกับการรักษาความเป็นส่วนตัวและการระวังอันตรายบนโลกอินเทอร์เน็ตที่จะเกิดกับหน่วยงานและตนเอง