บทที่ 3
การวิเคราะห์และออกแบบระบบ

3.1 การวิเคราะห์ระบบเดิม

การที่หลายฝ่ายตระหนักถึงปัญหาของภัยคุกคามเยาวชนที่เกิดขึ้นจากเนื้อหาบนอินเทอร์เน็ต จึงได้มีการผลิตโปรแกรมในรูปแบบต่างๆ กัน เพื่อป้องกันและแก้ไขปัญหานี้ โดยผู้ศึกษาได้ ทำการวิเคราะห์ระบบระบบควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต ซึ่งมีอยู่ในปัจจุบัน พบว่ายังมีความไม่สมบูรณ์อยู่ในหลายประเด็น พอจะจำแนกออกเป็นข้อๆ ได้ดังนี้

1) โปรแกรมถูกติดตั้งไว้ในเครื่องผู้ใช้ ทำให้การปรับเปลี่ยนรูปแบบหรือการตั้งค่าต่างๆ ในการป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต ต้องกระทำที่ตัวเครื่องนั้นๆ เท่านั้น ในกรณีที่ผู้ปกครองไม่ได้อยู่ที่บ้าน การปรับตั้งค่าต่างๆ จะเป็นไปไม่ได้เลย ทำให้การทำงานของระบบป้องกันและควบคุมเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต ไม่สามารถกระทำได้สะดวกและทันเวลา (Real Time)

2) มีการกำหนดเว็บไซต์ที่ป้องกันการเข้าถึงไว้ล่วงหน้า ระบบนี้ จะมีผู้ดูแลระบบ (Admin) เป็นผู้กำหนดชื่อของเว็บไซต์ที่จะป้องกันไม่ให้เยาวชนเข้าถึงเนื้อหาไว้ก่อน โดยจะมีการปรับปรุงรายการบัญชีชื่อเว็บไซต์ที่ต้องห้าม ใน ทุกครั้งที่ผู้ใช้ทำการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ต อย่างไรก็ตามข้อเสียของระบบนี้คือเยาวชนจะถูกควบคุมการเข้าถึงเนื้อหาที่เหมือนกันหมด โดยไม่มีการแบ่งแยกตามความเหมาะสมของเนื้อหากับอายุ เนื่องจาก ผู้ดูแลระบบ จะเป็นคนเลือกและกลั่นกรองเนื้อหาของเว็บไซต์ด้วยวิธีการ ของตนเอง ทำให้เยาวชนอาจพลาดโอกาสการเข้าถึงเนื้อหาที่เป็นประโยชน์ได้

3) การจำกัดเวลา (Time Limit) ที่ตัวเครื่องของผู้ใช้ (Client) โดยระบบนี้จะมีการกำหนดเวลาเพื่อควบคุมให้ผู้ใช้เข้าถึงเนื้อหาในอินเทอร์เน็ตได้ตามเวลาที่ตั้งค่าไว้ โดยจะอ้างอิงกับเวลาที่อยู่ในระบบของเครื่องของผู้ใช้ เป็นเกณฑ์ ซึ่งผู้ใช้หรือเยาวชน สามารถเข้าไปปรับเวลาในตัวเครื่องนั้น เพื่อให้สามารถเข้าไปใช้ระบบอินเทอร์เน็ตได้อย่างต่อเนื่อง และเป็นผลให้ระบบการตั้งเวลาไม่สามารถทำงานได้อย่างสมบูรณ์ถูกต้องการวัตถุประสงค์ อีกทั้งผู้ปกครองก็ไม่สามารถที่จะปรับเปลี่ยนการตั้งเวลาต่างๆ ได้ ถ้าผู้ปกครองไม่ได้อยู่ที่หน้าเครื่องของผู้ใช้

4) การตรวจสอบเว็บไซต์ที่ผู้ใช้เข้าเยี่ยมชม ไม่สามารถทำได้ผ่านระบบเครือข่ายอินเทอร์เน็ต ในกรณีที่ผู้ปกครองไม่ได้อยู่ร่วมกันกับเยาวชนในสถานที่ ที่เครื่องคอมพิวเตอร์นั้นๆ ตั้งอยู่ จะไม่สามารถเรียกดูข้อมูลการเข้าใช้อินเทอร์เน็ตของเยาวชนได้เลย จำเป็นต้องเดินทางกลับมาที่บ้านเพื่อเข้าไปตรวจสอบที่ตัวเครื่องคอมพิวเตอร์ของผู้ใช้ก่อนจึงจะสามารถเรียกดูประวัติการใช้งานต่างๆ ได้ ซึ่งทำให้การควบคุมและป้องกันภัยจากเนื้อหาบนอินเทอร์เน็ตเป็นไปได้ด้วยความล่าช้า

5) ไม่สามารถกำหนดสิทธิ์ของผู้ใช้ที่หลากหลายในเครื่องเดียวกันได้ ในกรณีที่ครอบครัวนั้นมีบุตรหรือเยาวชนมากกว่า 1 คน โดยแต่ละคนมีอายุ เพศ ระดับการศึกษา และวุฒิภาวะ แตกต่างกันมาก แต่มีเครื่องคอมพิวเตอร์ที่ใช้งานร่วมกันเพียงเครื่องเดียว ทำให้การกำหนดสิทธิ์การเข้าถึงเนื้อหาที่แตกต่างกันไม่สามารถทำได้ เนื่องจากใช้โปรแกรมตัวเดียวกัน มีการป้องกันหรือควบคุมเนื้อหาแบบเดียวกันทั้งหมด ไม่ได้สนับสนุนระบบผู้ใช้งานหลายคน (MultiUser)

6) ไม่สนับสนุนการกลั่นกรองชื่อเว็บไซต์ภาษาต่างประเทศ ในกรณีที่เยาวชนหรือผู้ใช้งานใช้ภาษาอื่นๆ นอกจากภาษาอังกฤษ เช่นภาษาฝรั่งเศส จีน หรือ เยอรมัน เพื่อเข้าถึงเว็บไซต์ที่มีเนื้อหาที่ไม่เหมาะสมนั้น ระบบจะไม่สามารถทำการกลั่นกรองใดๆ ได้เลย เนื่องจากไม่สามารถออกแบบเพื่อให้เข้าใจความหมายครอบคลุมได้ทุกๆ ภาษาในโลกนี้

จะเห็นได้ว่า ปัจจุบัน ระบบป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ตนั้น ยังมีข้อจำกัดในการใช้งานอยู่อีกมาก ทำให้การป้องกันและควบคุมเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมนั้น เป็นไปอย่างไม่เต็มประสิทธิภาพและไม่เท่าทันกับเนื้อหาที่ไม่เหมาะสมทางอินเทอร์เน็ต ที่มีการเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลา ผู้ศึกษาจึงได้ออกแบบระบบป้องกันและควบคุมการเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต โดยคำนึงถึงข้อจำกัดต่างๆ ดังกล่าวและดำเนินการแก้ไขปรับปรุงเพื่อให้ได้ระบบ ป้องกันและควบคุมเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสม ที่มีประสิทธิภาพ และเป็นประโยชน์กับประเทศชาติต่อไป

3.2 แนวคิดในการออกแบบระบบ

ผู้ศึกษา ทำการออกแบบระบบให้มีการทำงานตามขั้นตอนดังกล่าวข้างต้น ก็ด้วยมีความเชื่อว่า การป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมทางอินเทอร์เน็ตนั้น ไม่สามารถปล่อยให้เป็นภาระของสังคม หรือ หน่วยงานใดๆ ของรัฐได้ โดยไม่มีการร่วมมือของครอบครัว ซึ่งถือว่าเป็นหน่วยสังคมที่มีความสำคัญและ ใกล้ชิดกับเยาวชนมากที่สุด ดังนั้น แนวคิดในการออกแบบระบบ จึงตั้งอยู่บนพื้นฐานดังต่อไปนี้

(1) ผู้ปกครองต้องมีส่วนร่วมในการควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต

(2) ผู้ปกครองและผู้ดูแลระบบ จะต้องสามารถควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต ได้อย่างรวดเร็ว ทันเวลา (Real Time) และสามารถทำได้จากทุกที่ทุกเวลาผ่านทางระบบอินเทอร์เน็ต

ผู้ปกครองและเยาวชนผู้ใช้ต้องสามารถใช้งานระบบได้โดยง่าย และ ผู้ดูแลระบบสามารถที่จะช่วยเหลือผู้ปกครองในการป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ตได้

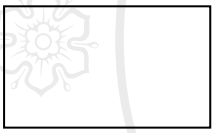
3.3 การออกแบบระบบใหม่

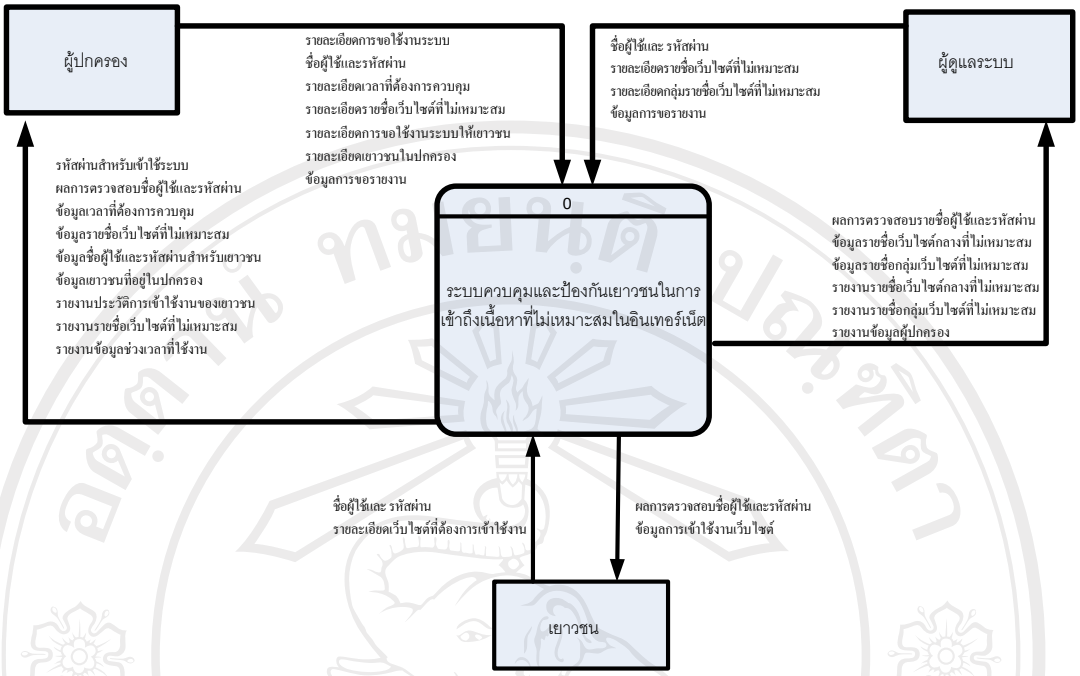
การวิเคราะห์และออกแบบระบบควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ตนั้น มีการใช้เครื่องมือในการวิเคราะห์และออกแบบระบบดังนี้

(1) แผนผังบริบท (Context diagram) เป็นแผนผังที่แสดงถึงภาพรวมของระบบและความสัมพันธ์กับสิ่งแวดล้อมที่เกี่ยวข้อง

(2) แผนภาพกระแสข้อมูล (Data flow diagram) หรือ DFD เป็นแผนภาพแสดงให้เห็นลักษณะเชิงกายภาพของระบบ

ตาราง 3.1 แสดงสัญลักษณ์ที่ใช้ในการออกแบบระบบ

สัญลักษณ์	ชื่อ	ความหมาย
	กรรมวิธี (process)	สัญลักษณ์ของการประมวลผลที่เกิดขึ้นในระบบหรือส่วนที่ทำให้ข้อมูลมีการเปลี่ยนแปลง
	ที่เก็บข้อมูล (data store)	ส่วนที่เก็บข้อมูล สามารถใช้แทนสิ่งต่างๆ ที่เป็นการจัดเก็บข้อมูลได้
	แหล่งกำเนิดข้อมูล (source) / แหล่งสารสนเทศ (sink) ของระบบ	เป็นต้นกำเนิดและ/หรือจุดปลายทางของข้อมูล
	ตัวแปรภายนอก (External Entity)	ใช้แทนแหล่งกำเนิดข้อมูลที่แสดงซ้ำกันหลายแห่งในแผนผัง
	กระแสข้อมูล (data flow)	แสดงถึงการเคลื่อนที่ของข้อมูลในระบบ จากที่หนึ่งไปยังอีกที่หนึ่ง



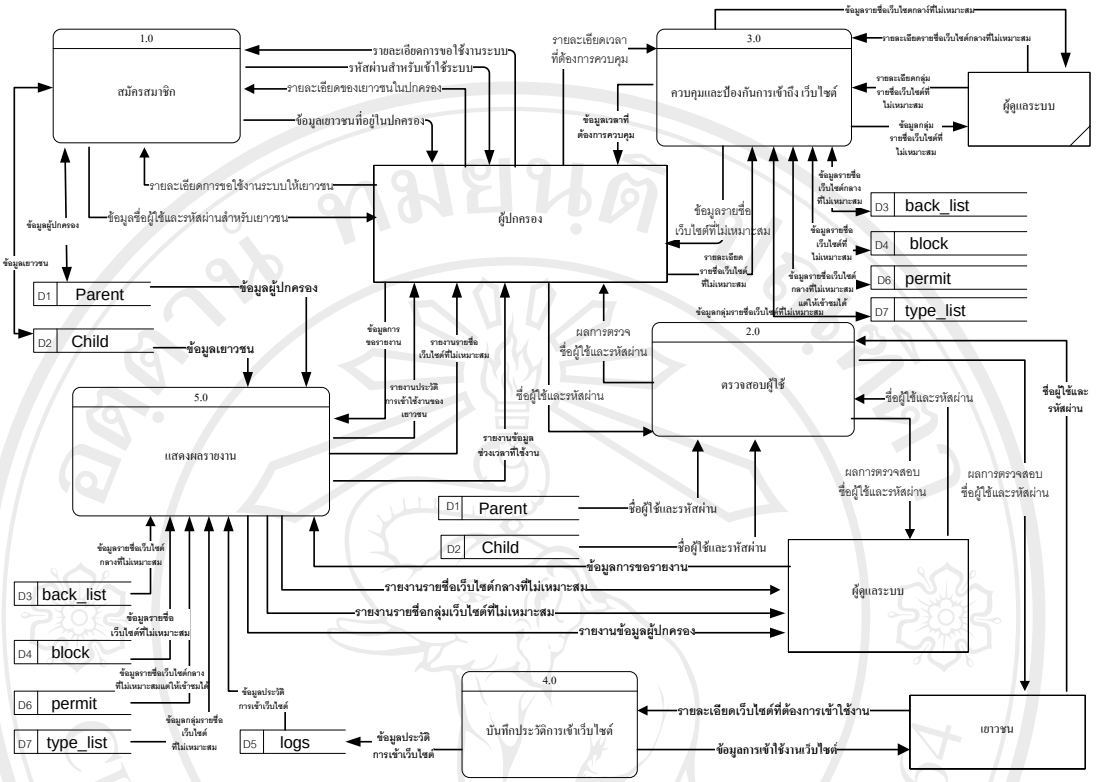
รูป 3.1 แผนผังบริบทของระบบควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต

จากรูป 3.1 เป็นแผนผังบริบทของระบบควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต โดยมีผู้เกี่ยวข้องคือ ผู้ดูแลระบบ ผู้ปกครอง และเยาวชน โดยจะทำงานสัมพันธ์กันดังต่อไปนี้

(1) ผู้ดูแลระบบ ขอบเขตการทำงานในระบบคือ กำหนด เพิ่ม แก้ไข และลบ กลุ่มรายชื่อเว็บไซต์ที่ไม่เหมาะสม กำหนด เพิ่ม แก้ไข และลบ รายชื่อเว็บไซต์ที่ไม่เหมาะสม รวมทั้งสามารถแก้ไข ลบ และ ส่งรหัสผ่านใหม่ให้กับผู้ปกครองที่ได้ลงทะเบียนไว้ในระบบ

(2) ผู้ปกครอง ขอบเขตการทำงานในระบบคือ กำหนดรายชื่อและรายละเอียดของเยาวชน กำหนดรายชื่อเว็บไซต์ที่ไม่เหมาะสมกับเยาวชนแต่ละคน กำหนดช่วงเวลาที่อนุญาตให้เยาวชนเข้าใช้อินเทอร์เน็ต ตรวจดูประวัติการเข้าใช้อินเทอร์เน็ตของเยาวชน

(3) เยาวชน ขอบเขตการทำงานในระบบคือ สามารถเข้าชมเว็บไซต์ที่ผู้ปกครองกำหนดสิทธิ์อนุญาตไว้ในระบบ



รูป 3.2 แสดงแผนภาพกระแสข้อมูล ระดับที่ 0

จากรูป 3.2 แผนภาพกระแสข้อมูลของระบบควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต ระดับที่ 0 สามารถแยกกระบวนการของระบบออกเป็นกระบวนการย่อยๆ ได้ทั้งหมด 5 กระบวนการดังนี้

กระบวนการ 1.0 กระบวนการสมัครสมาชิก เป็นกระบวนการสมัครเข้าใช้บริการและขอชื่อผู้ใช้และรหัสผ่านสำหรับผู้ปกครอง และเยาวชน

กระบวนการ 2.0 กระบวนการตรวจสอบผู้ใช้ เป็นกระบวนการสำหรับการตรวจสอบตัวตนของผู้ใช้แต่ละรายได้แก่ ชื่อผู้ใช้และรหัสผ่านของ ผู้ดูแลระบบ ผู้ปกครอง และเยาวชน โดยเมื่อแต่ละคนเข้าสู่กระบวนการนี้ ระบบจะทราบได้ว่า ผู้ใช้ที่เข้ามาในระบบนี้คือใคร

กระบวนการ 3.0 กระบวนการควบคุมและป้องกันการเข้าถึงเว็บไซต์ เป็นกระบวนการสำหรับการควบคุมและป้องกันเยาวชนจากการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม โดยจะทำการควบคุมและป้องกันเยาวชนตามสิทธิ์ที่ถูกกำหนดไว้ในระบบแล้วโดยผู้ปกครองหรือผู้ดูแลระบบ

กระบวนการ 4.0 กระบวนการบันทึกประวัติการเข้าเว็บไซต์ เป็นกระบวนการที่จะจัดเก็บข้อมูลรายชื่อพร้อมวันและเวลาที่เยาวชนแต่ละคนเข้าไปในแต่ละเว็บไซต์

กระบวนการ 5.0 กระบวนการแสดงผลรายงาน เป็นกระบวนการสำหรับแสดงผลรายงานต่างๆ โดยผู้ปกครองและผู้ดูแลระบบสามารถเลือกเงื่อนไขในการออกรายงานได้

3.4 การออกแบบฐานข้อมูล

จากการรวบรวมข้อมูล สามารถนำมาสร้างเป็นฐานข้อมูลได้ ในตาราง 3.2 ดังนี้

ตาราง 3.2 แสดงตารางข้อมูลทั้งหมดของระบบฐานข้อมูล

ลำดับ	ชื่อตาราง	ประเภท	รายละเอียด
1	parent ข้อมูลผู้ปกครอง	Master table	เก็บข้อมูลรายละเอียดเกี่ยวกับผู้ปกครอง
2	child รายละเอียดเยาวชน	Master table	เก็บข้อมูลรายชื่อเยาวชนพร้อมสิทธิ์ต่างๆ ที่ผู้ปกครองกำหนดไว้
3	back_list เว็บไซต์ที่ไม่เหมาะสมส่วนกลาง	Transaction table	เก็บข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมส่วนกลาง
4	block เว็บไซต์ไม่เหมาะสมครอบครัว	Transaction table	เก็บข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมของแต่ละครอบครัว
5	logs ประวัติการเข้าใช้	Transaction table	เก็บข้อมูลประวัติการเข้าชมเว็บไซต์ของเยาวชน
6	permit อนุญาตเข้าเว็บไซต์ไม่เหมาะสม	Transaction table	เก็บข้อมูลรายชื่อเว็บไซต์ไม่เหมาะสมส่วนกลางที่ผู้ปกครองอนุญาตให้เยาวชนเข้าชมได้
7	type_list กลุ่มรายชื่อเว็บไซต์ไม่เหมาะสม	Reference table	เก็บข้อมูลชื่อกลุ่มของเว็บไซต์ที่ไม่เหมาะสม

โครงสร้างฐานข้อมูล

โครงสร้างฐานข้อมูลของระบบควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ต เก็บภายใต้โปรแกรมฐานข้อมูล มายเอสคิวแอล (MySQL) โดยใช้ภาษาแอสคิวแอล (SQL) ในการจัดการฐานข้อมูล มีลักษณะแบบของข้อมูล (Data type) ดังนี้

ตาราง 3.3 แสดงแบบของข้อมูล

ข้อมูลชนิดตัวเลข		
ประเภท	ขนาดที่จัดเก็บ	ค่าที่จัดเก็บ
INT หรือ INTEGER	4 ไบต์	เป็นค่าจำนวนเต็มขนาดปกติ ถ้าเป็นค่าบวกอย่างเดียว (unsigned) จะมีค่าตั้งแต่ 0 ถึง 4294967295 แต่ถ้าเป็นค่าบวกและลบ (signed) จะมีค่าตั้งแต่ –2147483648 ถึง 2147483647
ข้อมูลประเภทวันที่		
ประเภท	ขนาดที่จัดเก็บ	ค่าที่จัดเก็บ
TIME	3 ไบต์	เก็บวันที่และเวลาในรูปแบบ ค.ศ.-เดือน-วัน ชั่วโมง-นาที-วินาที (YYYY-MM-DD HH:MM:SS) โดยมีค่าตั้งแต่ 0001-01-01 00:00:00 ถึง 9999-12-31 23:59:59
DATETIME	8 ไบต์	เก็บวันที่และเวลาในรูปแบบ ค.ศ.-เดือน-วัน ชั่วโมง-นาที-วินาที (YYYY-MM-DD HH:MM:SS) โดยมีค่าตั้งแต่ 0001-01-01 00:00:00 ถึง 9999-12-31 23:59:59
ข้อมูลประเภทตัวอักษร		
ประเภท	ขนาดที่จัดเก็บ	ค่าที่จัดเก็บ
VARCHAR (M)	ขนาดตามข้อมูลจริง แต่ไม่เกิน 255 ไบต์	อักษรตามรหัส ascii

จากตาราง 3.3 สามารถนำลักษณะแบบข้อมูล มาออกแบบตารางฐานข้อมูลเพื่อจัดเก็บข้อมูลของระบบควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ตได้ดังนี้

1) ตาราง parent ทำหน้าที่จัดเก็บข้อมูลรายละเอียดเกี่ยวกับผู้ปกครอง รายละเอียดดังแสดงไว้ในตาราง 3.4

ตาราง 3.4 แสดงรายละเอียดตารางข้อมูลรายละเอียดเกี่ยวกับผู้ปกครอง

ชื่อตาราง : parent คำอธิบาย : เก็บข้อมูลรายละเอียดเกี่ยวกับผู้ปกครอง คีย์หลัก (primary key) : parent_id			
ชื่อเขตข้อมูล	ชนิดและขนาด(ไบต์)	คำอธิบาย	ตัวอย่างข้อมูล
parent_id	int(4)	หมายเลขผู้ปกครอง	1
parent_name	varchar(50)	ชื่อผู้ปกครอง	ณรงค์ ชีวานันท์
parent_address	text	ที่อยู่	22/234 ถ.มณีนพรัตน์..
parent_tel	varchar (20)	เบอร์โทรศัพท์	0897655089
parent_email	varchar(30)	อีเมล์	fifa@gmail.com
parent_user	varchar(20)	ชื่อผู้ใช้	narong
parent_pass	varchar(8)	รหัสผ่าน	123456

2) ตาราง child ทำหน้าที่จัดเก็บข้อมูลรายชื่อเยาวชนพร้อมสิทธิ์ต่างๆ ที่ผู้ปกครองกำหนดไว้ รายละเอียดดังแสดงไว้ใน ตาราง 3.5

ตาราง 3.5 แสดงรายละเอียดตารางข้อมูลรายชื่อเยาวชนพร้อมสิทธิ์ต่างๆ ที่ผู้ปกครองกำหนดไว้

ชื่อตาราง : child คำอธิบาย : เก็บข้อมูลรายชื่อเยาวชนพร้อมสิทธิ์ต่างๆ ที่ผู้ปกครองกำหนดไว้ คีย์หลัก (primary key) : child_id			
ชื่อเขตข้อมูล	ชนิดและขนาด(ไบต์)	คำอธิบาย	ตัวอย่างข้อมูล
child_id	int(4)	หมายเลขเยาวชน	2
child_name	varchar(50)	ชื่อของเยาวชน	พศิกา
child_user	varchar(20)	ชื่อผู้ใช้ของเยาวชน	pasika
child_password	varchar(8)	รหัสผ่านของเยาวชน	12345678
parent_id	int(4)	หมายเลขผู้ปกครอง	1
time_start	time(3)	เวลาเริ่มต้นที่อนุญาต	09:00:00
time_end	time(3)	เวลาสิ้นสุดที่อนุญาต	23:00:00
time_login	varchar(30)	เวลาที่เยาวชนเริ่มเข้าสู่ระบบ	1700

3) ตาราง back_list ทำหน้าที่จัดเก็บข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมส่วนกลาง ดังรายละเอียดแสดงไว้ในตาราง 3.6

ตาราง 3.6 แสดงรายละเอียดตารางข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมส่วนกลาง

ชื่อตาราง : back_list คำอธิบาย : เก็บข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมส่วนกลาง คีย์หลัก (primary key) : back_list_id			
ชื่อเขตข้อมูล	ชนิดและขนาด(ไบต์)	คำอธิบาย	ตัวอย่างข้อมูล
back_list_id	int(4)	หมายเลขเว็บไซต์ที่ไม่เหมาะสมส่วนกลาง	1
back_list_url	varchar(50)	รายชื่อเว็บไซต์ที่ไม่เหมาะสมส่วนกลาง	www.sexy.com
type_name	varchar(30)	รายชื่อกลุ่มของเว็บไซต์ที่ไม่เหมาะสม	Nudity

4) ตาราง block ทำหน้าที่จัดเก็บข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมของแต่ละครอบครัว ดังรายละเอียดแสดงไว้ใน ตาราง 3.7

ตาราง 3.7 แสดงรายละเอียดตารางข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมของแต่ละครอบครัว

ตาราง : block คำอธิบาย : เก็บข้อมูลเว็บไซต์ที่ไม่เหมาะสมของแต่ละครอบครัว คีย์หลัก (primary key) : block_id			
ชื่อเขตข้อมูล	ชนิดและขนาด(ไบต์)	คำอธิบาย	ตัวอย่างข้อมูล
block_id	int(4)	หมายเลขเว็บไซต์ที่ไม่เหมาะสมของครอบครัว	1
block_url	varchar(50)	รายชื่อเว็บไซต์ที่ไม่เหมาะสมของครอบครัว	www.thaisex.com
child_id	int(4)	หมายเลขของเยาวชน	1
parent_id	int(4)	หมายเลขของผู้ปกครอง	3

5) ตาราง logs ทำหน้าที่จัดเก็บข้อมูลประวัติการเข้าชมเว็บไซต์ของเยาวชน ดังรายละเอียดแสดงไว้ในตาราง 3.8

ตาราง 3.8 แสดงรายละเอียดตารางข้อมูลประวัติการเข้าชมเว็บไซต์ของเยาวชน

ชื่อตาราง : logs คำอธิบาย : เก็บข้อมูลประวัติการเข้าชมเว็บไซต์ของเยาวชน คีย์หลัก (primary key) : logs_id			
ชื่อเขตข้อมูล	ชนิดและขนาด(ไบต์)	คำอธิบาย	ตัวอย่างข้อมูล
logs_id	int(4)	หมายเลขประวัติ	155
logs_url	varchar(50)	ชื่อเว็บไซต์ที่อยู่ในประวัติ	www.sex.com
logs_date	datetime(8)	วันที่และเวลาที่เข้าชม	2007-09-16 4:19:11
child_id	int(4)	หมายเลขเยาวชน	2
logtype	int(4)	ประเภทประวัติการเข้าชม	0

อธิบายรหัสประเภทของประวัติการเข้าชมเว็บไซต์ (logtype) ได้ดังนี้

0 คือ เว็บไซต์ที่มีเนื้อหาที่ไม่เหมาะสมหรือไม่ได้รับอนุญาตให้เข้าชม

1 คือ เว็บไซต์ที่มีเนื้อหาเหมาะสมหรือได้รับอนุญาตให้เข้าชม

6) ตาราง permit ทำหน้าที่จัดเก็บข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมส่วนกลางที่ผู้ปกครองอนุญาตให้เยาวชนเข้าชมได้ ดังรายละเอียดแสดงไว้ในตาราง 3.9

ตาราง 3.9 แสดงรายละเอียดตารางข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมส่วนกลาง

ชื่อตาราง : permit คำอธิบาย : เก็บข้อมูลรายชื่อเว็บไซต์ที่ไม่เหมาะสมส่วนกลางที่ผู้ปกครองอนุญาตให้เยาวชนเข้าชมได้ คีย์หลัก (primary key) : permit_id			
ชื่อเขตข้อมูล	ชนิดและขนาด(ไบต์)	คำอธิบาย	ตัวอย่างข้อมูล
permit_id	Auto increment	หมายเลขอนุญาต	1
back_list_id	int(4)	หมายเลขเว็บไซต์ที่ไม่เหมาะสมส่วนกลาง	2
child_id	int(4)	หมายเลขเยาวชน	3

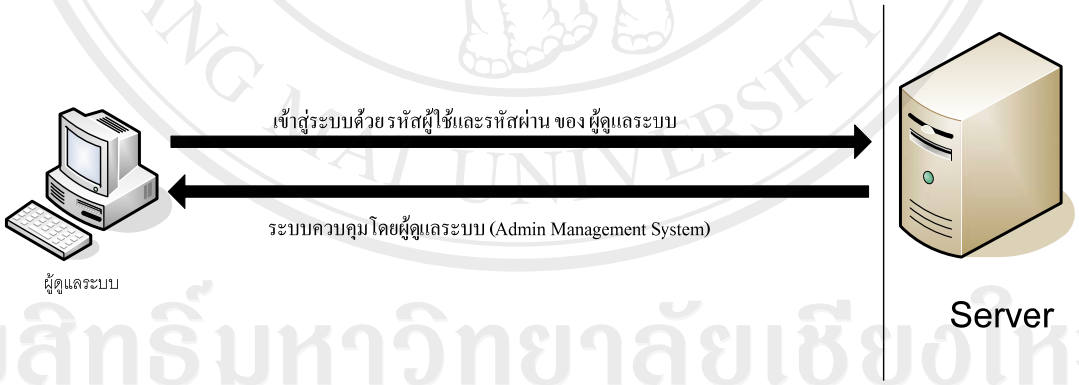
7) ตาราง type_list ทำหน้าที่จัดเก็บข้อมูลชื่อกลุ่มของเว็บไซต์ที่ไม่เหมาะสม ดังรายละเอียดแสดงไว้ในตาราง 3.10

ตาราง 3.10 แสดงรายละเอียดตารางข้อมูลชื่อกลุ่มของเว็บไซต์ที่ไม่เหมาะสม

ชื่อตาราง : type_list คำอธิบาย : เก็บข้อมูลชื่อกลุ่มของเว็บไซต์ที่ไม่เหมาะสม คีย์หลัก (primary key) : type_id			
ชื่อเขตข้อมูล	ชนิดและขนาด(ไบต์)	คำอธิบาย	ตัวอย่างข้อมูล
type_id	Auto increment	หมายเลขกลุ่มของเว็บไซต์ที่ไม่เหมาะสม	5
type_name	varchar(30)	รายชื่อกลุ่มของเว็บไซต์ที่ไม่เหมาะสม	Violence

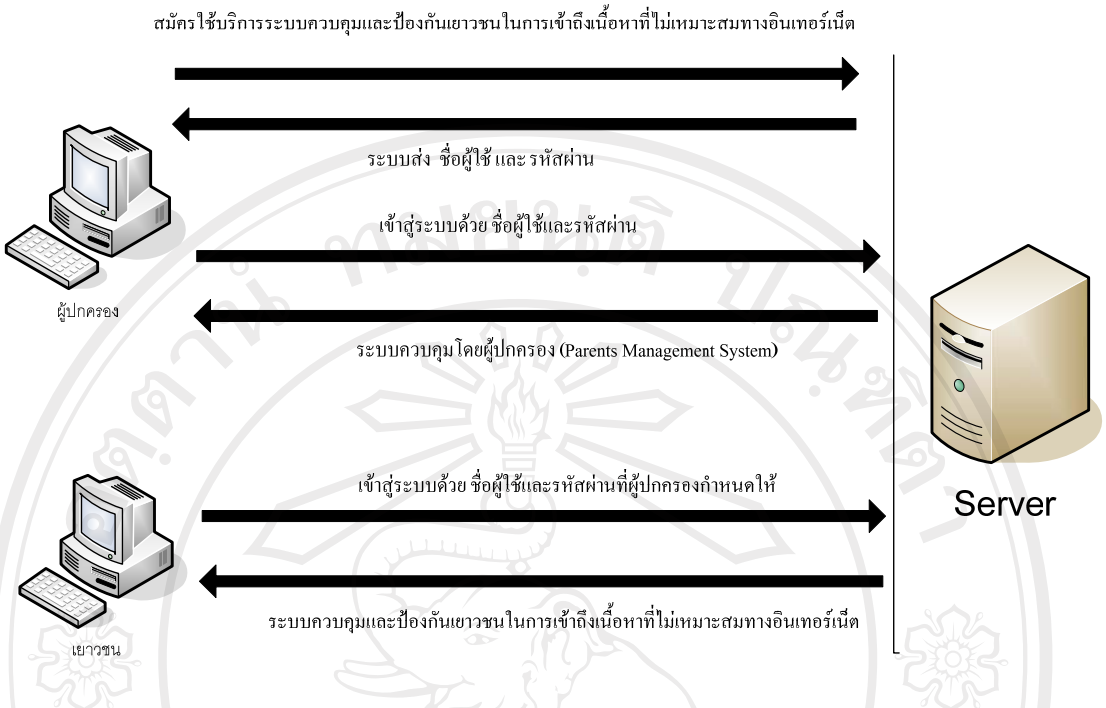
3.5 ภาพรวมของการทำงานระบบ

สำหรับขั้นตอนการทำงานของระบบควบคุมและป้องกันเยาวชนในการเข้าถึงเนื้อหาที่ไม่เหมาะสมในอินเทอร์เน็ตนั้น สามารถแสดงออกได้ในภาพรวมของระบบดังต่อไปนี้



รูป 3.3 แสดงภาพรวมการทำงานของระบบในส่วนของผู้ดูแลระบบ

เริ่มจากในส่วนของผู้ดูแลระบบจะ สามารถเข้าสู่ระบบผ่านทางหน้าเว็บเบราว์เซอร์ โดยใส่รหัสผู้ใช้ (User Name) และ รหัสผ่าน (Password) จากนั้นจะเข้าสู่ ระบบควบคุมโดยผู้ดูแลระบบ (Admin Management System) ซึ่งทำให้ผู้ดูแลระบบสามารถเรียกดูรายชื่อพร้อมรายละเอียดของผู้ปกครองทั้งหมดที่มีอยู่ในระบบ กำหนดกลุ่มของเว็บไซต์ที่ไม่เหมาะสม (Group Black List) และกำหนดรายชื่อ เว็บไซต์ที่ไม่เหมาะสมได้ (URL Black List)



รูป 3.4 แสดงภาพรวมการทำงานของระบบในส่วนของผู้ปกครองและเยาวชน

ขั้นตอนที่ 1

ผู้ปกครองแจ้งความจำนง ขอใช้บริการ ระบบ โดยกรอกรายละเอียดผ่านทางเว็บเบราว์เซอร์ แล้วส่ง ไปยัง เครื่องแม่ข่าย (Server) ระบบจะส่ง ชื่อผู้ใช้ (User Name) และ รหัสผ่าน (Password) กลับไปยัง ผู้ปกครอง

ขั้นตอนที่ 2

ผู้ปกครองนำ ชื่อผู้ใช้ และ รหัสผ่าน ของตน เข้าสู่ ระบบควบคุมโดยผู้ปกครอง (Parent Management System) ซึ่งระบบนี้จะอนุญาตให้ผู้ปกครองสามารถ เข้าไปกำหนดชื่อ รหัสผ่าน ของเยาวชนที่ตนต้องการให้อยู่ในระบบ กำหนดช่วงเวลาให้เยาวชนแต่ละคนสามารถเข้าใช้อินเทอร์เน็ต กำหนดรายชื่อเว็บไซต์ที่ไม่อนุญาตให้เยาวชนเข้าถึงเนื้อหา รวมทั้งสามารถตรวจสอบดูประวัติการเข้าเว็บไซต์ของเยาวชนย้อนหลังได้

ขั้นตอนที่ 3

ก่อนที่เยาวชนจะเริ่มต้นเข้าใช้งานอินเทอร์เน็ต เยาวชนจะต้องระบุ ชื่อผู้ใช้ และ รหัสผ่าน ของตน ถ้ารหัสผ่าน ถูกต้อง ระบบควบคุมและป้องกันการเข้าถึงเนื้อหาที่ไม่เหมาะสม จะเริ่มต้นทำงานทันที โดยจะอนุญาตให้เยาวชนเข้าสู่ เว็บเบราว์เซอร์ ได้ เมื่อเข้าสู่เว็บเบราว์เซอร์ได้แล้วเยาวชนจะระบุชื่อเว็บไซต์ที่ตนต้องการเข้าชม ถ้าเว็บนั้นถูกระบุอยู่ในบัญชีต้องห้ามที่ผู้ปกครองได้กำหนดไว้ล่วงหน้าแล้ว เยาวชนจะไม่สามารถเข้าสู่เนื้อหาในเว็บไซต์นั้นได้ โดยระบบจะแจ้งเตือนให้เยาวชนทราบผ่านทางหน้าเว็บไซต์ ในกรณีกลับกันถ้าเว็บนั้นไม่ได้เป็นเว็บต้องห้าม เยาวชนก็สามารถเข้าใช้งานอินเทอร์เน็ตได้ตามปกติ