Política General G07
Uso de la Red de Tecnología de la Información y Política de Correo Electrónico.

1. Declaración de la Política.

Esta política permite el uso aprobado, legal y eficiente de los servicios de correo electrónico e Internet en los campus de SAE Institute en Europa, en operaciones territoriales con licencia y en todos los campus de SAE que ofrecen programas en colaboración con la Universidad de Middlesex, y establece los estándares que se aplican al uso de la red de Tecnología de la Información (TI) y sistemas de comunicación por computadora y por correo electrónico.

2. Propósito.

Esta política tiene como objetivo garantizar el uso adecuado y legal de la red de Tecnología de la Información (TI) de SAE y los sistemas de comunicación por correo electrónico y por computadora. La política proporciona información específica sobre lo que SAE Institute considera el uso aceptable e inaceptable de estos servicios.

3. Alcance.

Esta política se aplica a todas las operaciones de SAE Institute en Europa, en operaciones territoriales con licencia y en todos los Campus que ofrecen programas en colaboración u operaciones con Universidad de Middlesex, y se aplica a todos los usuarios de cualquier sistema de TI o cualquier sistema de comunicación a través de la computadora o cualquier otro dispositivo electrónico. Todo el personal, los estudiantes y los usuarios invitados deben cumplir con las disposiciones de esta política al utilizar cualquiera de los sistemas proporcionados por el Instituto SAE.

Esta política se aplica a todos los usuarios independientemente de su ubicación, cuando utilizan equipos SAE (computadoras, laptops, etc.) o utilizan sistemas SAE para comunicarse (por ejemplo, por correo electrónico), o están conectados a la red SAE de forma remota o cuando acceden a la red SAE o enviar por correo electrónico los sistemas de TI en equipos que no pertenecen a SAE.

4. Políticas y Documentos Asociados.

Esta política debe leerse junto con las siguientes políticas y documentos:

- Código de Conducta G01
- Política de Información Pública G02
- Política de Privacidad de la Información G06.

5. Política.

5.1. Principios.

La red de TI, los sistemas de comunicación por computadora y por correo electrónico se proporcionan a los estudiantes para facilitar sus estudios y permitir el acceso al aprendizaje en línea y al material de investigación.

La red informática, los sistemas informáticos y los sistemas de comunicación por correo electrónico se proporcionan a todo el personal de SAE (contratados por tiempo parcial, en tiempo completo o en cualquier empleo o capacidad contractual) para facilitar sus actividades y resultados relacionados con el trabajo en SAE Institute.
Se proporciona y fomenta el uso adecuado de todos estos sistemas para ayudar al personal y los estudiantes en su trabajo, para mejorar la implementación de tecnologías modernas y emergentes para crear mayores eficiencias, mejor uso del tiempo en el trabajo, mejor acceso a la información y datos de investigación, y modos de comunicación más efectivos.
Sin embargo, dichos Sistemas SAE deben utilizarse de acuerdo con esta política para proteger a SAE, a su personal y a sus estudiantes de los riesgos adversos que pueden derivarse del uso incorrecto o no aprobado de estos sistemas. Los usuarios no deben acceder a ningún sistema o cuenta, excepto aquellos para los que se les ha otorgado autorización formal.

6. Riesgos Potenciales.

Los ejemplos de riesgos significativos que pueden surgir de un uso inaceptable incluyen, entre otros, los siguientes:

- Violaciones de la confidencialidad en relación con el personal o los datos del estudiante
- Infracción de los derechos de propiedad intelectual
- Acoso, difamación o calumnia de individuos
- Introducción de malware (software malicioso), virus o spyware (software espía) en la red SAE
- Participación electrónica en actividades ilegales o criminales.

7. Uso y Comportamientos Inaceptables.

La visualización, descarga, escucha, publicación o circulación de cualquier material considerado inapropiado u ofensivo no está permitido.
Los siguientes comportamientos específicos son inaceptables y se considerarán como una mala conducta que podría dar lugar a la terminación de los estudios o al empleo:

- uso de cualquier medio electrónico de una manera que viole las disposiciones del Código de Conducta de SAE (Política G01);
- visitar sitios de Internet o hacer circular cualquier mensaje o material que incluya contenido obsceno, de odio, pornográfico, racista, sexista, discriminatorio, abusivo o malicioso;
- utilizar Internet o correos electrónicos para enviar material ofensivo, acosador, difamatorio a otros usuarios internos o externos al Instituto SAE;
- usar computadoras para cometer cualquier forma de fraude, piratería de software, películas o música o el uso de cualquier tipo de software o estructura de igual a igual o de torrente;
- participación en cualquier campaña electrónica destinada a dañar o desacreditar a individuos u organizaciones;
- descargar software comercial o cualquier material protegido por derechos de autor que pertenezca a terceros sin la debida autorización o licencia;
- piratería en áreas no autorizadas del Instituto SAE u otras organizaciones;
- publicar o difundir material difamatorio o falso sobre SAE Institute, compañeros de estudios o el personal en sitios de redes sociales, 'blogs' (revistas en línea), 'wikis' o cualquier otra forma de publicación en línea;
- realizar actividades deliberadas que desperdician el esfuerzo del personal o los recursos de la red;
- introducir cualquier forma de software malicioso en la red corporativa;
- uso que de alguna manera infringe los derechos razonables de otros miembros del personal o estudiantes;
- uso de la red o de los sistemas SAE para ganancia o beneficio personal no autorizado o no aprobado;
- el uso de software de mapeo de red, o paquetes de rastreo en cualquier segmento de la red SAE;
- el uso de cualquier software o sistema para sortear o evadir la seguridad de la red y el control de acceso.

8. Uso Personal.

Se permite el uso limitado de los sistemas SAE para comunicaciones personales por parte del personal o los estudiantes siempre que se mantenga estrictamente a un mínimo durante las horas de trabajo o los estudios formales, que no interfiera con los deberes laborales o las responsabilidades normales del personal o el trabajo académico del estudiante, que no interfiera con las actividades académicas

normales o las operaciones comerciales de SAE, y que el uso cumpla con las disposiciones de esta política.
Cuando un miembro del personal o un Gerente de línea tiene motivos para creer que un estudiante o miembro del personal está haciendo un uso privado irrazonable de los recursos de SAE, este permiso para uso personal puede ser retirado por el Administrador del Campus u otro miembro responsable del Personal Senior.

9. Monitoreo y Control.

Todos los recursos y sistemas electrónicos y relacionados con Internet se proporcionan con fines de estudio o para fines laborales. Para garantizar el cumplimiento normativo y legal, SAE Institute se reserva el derecho de supervisar y registrar el tráfico de Internet y de red, incluido el historial de navegación, junto con los sitios de Internet visitados de acuerdo con la legislación local. El contenido específico de cualquier transacción o comunicación electrónica normalmente no se supervisará a menos que existan motivos razonables para deducir un uso incorrecto o ilegal. Cualquier decisión para supervisar el contenido debe ser autorizada por el Administrador del Campus o un Director Senior.
Todos los correos electrónicos del personal y las comunicaciones enviadas o recibidas usando los Sistemas de Soporte Técnico IT se almacenan, y se puede acceder después de la aprobación de un Administrador Superior si es necesario. Ejemplos de propósitos autorizados pueden incluir:
• para detectar el uso no autorizado de los sistemas
• para proteger los sistemas contra el malware y la explotación
• para recuperar datos en caso de falla de la computadora
• para cumplir con la obligación legal
• para prevenir o detectar el crimen
• para investigar una queja seria.
Dicha información recopilada normalmente se almacenará durante al menos 1 año y no se compartirá con ninguna parte a menos que esté autorizada o exija una obligación legal.

10. Obligaciones de Inicio de Sesión.

Es responsabilidad de cada usuario garantizar que se mantenga la seguridad y confidencialidad de las credenciales de inicio de sesión, y revelar las contraseñas de acceso a personas no autorizadas en cualquier parte de las operaciones de SAE puede incurrir en medidas disciplinarias.
Las contraseñas de acceso deben ser seguras y cumplir con la política de contraseñas:

- a menos que se apruebe lo contrario, todas las contraseñas deben tener una longitud de 6 caracteres o más y contienen una combinación de al menos 2 de las siguientes opciones:
- •Letras mayúsculas
- Caracteres minúsculos
- •Números
- Caracteres no alfanuméricos.

No se permiten cadenas consecutivas de caracteres (por ejemplo, AbcdEfg o 1@345^ se consideran contraseñas débiles y no están permitidas)

11. Uso de Internet.

11.1. Descargando.

Los estudiantes no deben descargar programas de software, aplicaciones modificadas, música u otro contenido creativo o electrónico a ningún sistema de TI a menos que se haya otorgado permiso o se hayan emitido instrucciones específicas por parte del departamento de TI o un miembro del personal de SAE (por ejemplo, administrador, conferencista, o gerente).

11.2. Uso de Correo Electrónico.

El correo electrónico se almacenará, y se considera permanente (una publicación en un tribunal de justicia).
Se debe tener especial cuidado con la transmisión de información sensible o confidencial.
El envío de correos electrónicos desde cualquier cuenta de trabajo hace que esa persona sea un agente de SAE, y se debe tener cuidado de que cualquier comunicación se refleje bien en SAE Institute.
Se debe tener especial cuidado al abrir archivos adjuntos al correo electrónico en caso de propagación de software malicioso o cualquier virus. Cualquier estudiante o miembro del personal que crea que pudo haber contribuido a la propagación de un virus o malware debe notificarlo de inmediato al oficial de TI.
Se adjuntan más consejos y orientación sobre el uso del correo electrónico en los Apéndices A y B.

11.3. Sitios Web, Derechos de Autor y Redes Sociales.

El uso de cualquier sitio web de SAE está sujeto a los términos de esta política o de cualquier política contenida en los sitios web.
El personal debe asegurarse de que toda la información que se coloca en los sitios web de SAE sea correcta, completa y actual, que cumpla con todas las políticas

relevantes (especialmente la Política de Información Pública G02) y que haya sido aprobada por el Gerente correspondiente.
El personal debe asegurarse de que todo el material publicado en sitios web o redes sociales esté libre de derechos de autor, o que los derechos de autor sean propiedad de SAE, y que se haya obtenido el permiso correspondiente para cualquier material protegido por derechos de autor.
En el Apéndice A de la Política G02 sobre Información Pública encontrará más consejos y orientación sobre el uso de las redes sociales.

12. Estación de Trabajo y Seguridad de Red.

Las personas son responsables de garantizar la seguridad de su estación de trabajo asignada o computadora portátil, y deben asegurarse de que las personas no autorizadas no accedan a ellas.
Todas las estaciones de trabajo y laptops SAE deben tener el software con licencia vigente instalado y en ejecución, y el personal o los estudiantes no deben instalar o ejecutar ninguna aplicación que no haya sido aprobada por el responsable de TI o el administrador del campus.
La desconexión de todos los servicios y sitios web debe ocurrir al salir de una estación de trabajo para evitar el acceso no autorizado.
La red SAE no se debe usar para descargar, distribuir o acceder a materiales ilegales, ofensivos o con derechos de autor a menos que (en el caso de materiales protegidos por derechos de autor) el titular de los derechos de autor haya otorgado permiso para hacerlo.
El uso de software de intercambio de archivos punto a punto y sitios de descarga de enlaces directos (compartir rápido) está prohibido en cualquier red SAE.

13. Uso e Instalación del Software.

El uso del software está limitado por derechos de autor y licencias. Solo se debe utilizar el software instalado por el responsable de TI relevante bajo la autorización del Administrador del Campus y al que el usuario tiene permiso de acceso.
La copia o distribución de software sin autorización está estrictamente prohibida, y se debe solicitar y otorgar permiso previo antes de la instalación de cualquier software o complemento.
El personal o los estudiantes que trabajan en una laptop de SAE deben asegurarse de que todo el software instalado en la misma cuente con una licencia completa y cumpla con esta política.

14. Protección de Datos.

Se requiere que todo el personal cumpla con las disposiciones de la Política G06 sobre Privacidad de la Información, así como con la legislación local relacionada actual, y debe tomar todas las precauciones razonables para garantizar que la información privada relacionada con el personal o estudiantes se mantenga segura contra el acceso no autorizado.

15. Infracciones y Acción Disciplinaria.

Cualquier incumplimiento o incumplimiento de esta política se tratará como incumplimiento del Código de Conducta, es decir, como mala conducta, y puede dar lugar a procedimientos disciplinarios.