Política de Uso Aceptable de la tecnología de la información y la comunicación.

COLOMBIA

Septiembre de 2023

Política de Uso Aceptable de la tecnología de la información y la comunicación.

1 Objeto

1.1 Esta política define y describe el uso aceptable de la tecnología de la información y comunicación y teléfonos móviles para los empleados en los colegios. El objeto de la política es definir los estándares que deben mantener los empleados cuando usan los sistemas informáticos del colegio; minimizar los riesgos a estudiantes de contacto inapropiado por parte de los empleados; proteger a los empleados y a los colegios de demandas y minimizar el riesgo para los sistemas informáticos.

2 Aplicación

2.1 Esta política se refiere al uso de los equipos informáticos de los colegios del grupo Cognita y se aplica a todos los empleados de los colegios y otros usuarios autorizados, por ejemplo, proveedores y voluntarios.

2.2 Esta política no forma parte del contrato laboral de ningún empleado y Cognita se reserva el derecho de modificarla en cualquier momento. Sin perjuicio de lo anterior, el incumplimiento de esta política podrá derivar en un incumplimiento de las obligaciones contractuales asumidas por la persona, con las consecuencias que sean aplicables al caso.

3 responsabilidades del Colegio

3.1 Cognita - Redcol, como órgano de gobernación del colegio, tiene la responsabilidad de asegurar que sus empleados actúen de forma legal, haciendo un uso apropiado de la tecnología por motivos autorizados.

3.2 Cognita - Redcol tiene la responsabilidad de adoptar las políticas relevantes y el director del colegio es responsable de asegurar que el colegio adopte la política y el personal tenga conocimiento de su contenido.

3.3 El director es responsable de mantener un inventario de los equipos tecnológicos (hardware y software), que incluye equipos entregados a empleados para uso personal, como portátiles y teléfonos.

3.4 Si el director tiene motivo para pensar que cualquier equipo haya sido maltratado o utilizado para fines distintos de los autorizados, debe consultar con el responsable nacional de Informática, la coordinadora de salvaguarda y la vicepresidenta de educación sin demora. Ellos acordarán, con el director, una estrategia para investigar los hechos. Los incidentes se investigarán de acorde con los procedimientos de la empresa.

3.5 Los directores se asegurarán de que los empleados del colegio no realicen investigaciones por su cuenta al menos que se les autorice hacerlo.

4 Responsabilidades del usuario

4.1 El empleado que incumpla esta política podría ser objeto de un procedimiento disciplinario. En algunas circunstancias, el incumplimiento de esta política se podría considerar una falta muy grave y resultar en la terminación de un contrato laboral. Los usuarios deben informar al director de cualquier sospecha de incumplimiento de esta política.

4.2 Los usuarios y sus jefes directos son responsables de asegurar que el apoyo y la formación adecuada se lleven a cabo para poder implementar esta política.

4.3 Cuando acceden a los sistemas informáticos del colegio, los usuarios acuerdan cumplir esta Política de Uso Aceptable y otras políticas relacionadas.

4.4 Se espera que todos los usuarios actúen de manera responsable, ética y legal. Los usuarios deben cumplir con la legislación de protección de datos, La Constitución Política de Colombia estableció en el artículo 15 el derecho de protección de datos personales como el derecho de toda persona para conocer, actualizar, rectificar y/o cancelar la información y datos personales que de ella se hayan recolectado y/o se traten en

bases de datos públicas o privadas. Mediante la Ley 1581 del 17 de octubre de 2012, el Congreso de la República reglamentó el ya mencionado derecho al establecer las Disposiciones Generales para la Protección de Datos Personales en Colombia, igualmente reglamentada por los Decretos 1377 de 2013 y 886 de 2014 (hoy incorporados en el Decreto único 1074 de 2015), además de la política de Protección de Datos de Cognita y/o de Redcol, manteniendo la privacidad y confidencialidad, sobre todo la de los estudiantes. Se debe llevar cuidado de no incumplir los derechos de autor, marca registrada o diseño de otra persona, y de no publicar contenido difamatorio.

4.5 Los empleados firmarán la recepción de los equipos informáticos como portátiles y teléfonos. Los empleados usarán estos equipos solo para trabajos profesionales autorizados.

4.6 Los empleados seguirán los procedimientos autorizados cuando llevan los dispositivos móviles, propiedad del colegio, fuera del recinto.

4.7 Nadie puede usar los recursos informáticos en violación de los acuerdos de licencia, derechos de autor, contratos o leyes nacionales.

4.8 El personal debe proteger los dispositivos portátiles, con una contraseña de un mínimo de 6 caracteres y actualizar esta contraseña con frecuencia (cada trimestre).

4.9 Se requiere que los usuarios del sistema informático protejan sus contraseñas y no compartan detalles de sus cuentas, ni utilicen las cuentas de otros ni tergiversen su identidad. En ninguna circunstancia revelarán los usuarios sus contraseñas a otra persona.

4.10 Ningún usuario usará (por ejemplo, leer, escribir, modificar, eliminar, copiar o mover) los documentos personales de otro, sin el permiso de la otra persona al menos que lo permita esta política o la ley. Esto incluye el correo electrónico.

4.11 Los usuarios no deben subir ni descargar software sin la autorización del director. Se llevarán a cabo auditorias periódicas de los equipos informáticos.

4.12 Los usuarios no deben llevar datos personales (sobre todo datos relacionados con los estudiantes) fuera del colegio, sin la autorización del director. Datos electrónicos llevados fuera del colegio se deben proteger con contraseña y encriptación. Esto incluye datos contenidos en equipos portátiles (ordenadores portátiles, USB) y herramientas de sincronización de datos como Dropbox. Hay que tener especial cuidado si se usa los equipos informáticos fuera del lugar de trabajo y tomar medidas de vez en cuando para no importar virus o comprometer la seguridad del sistema. El sistema contiene información confidencial y/o sujeta a las leyes de protección de datos. Se debe tratar con sumo cuidado y de acuerdo con la política de Protección de Datos de Cognita.

4.13 Cualquier dispositivo que conecta a la red interna del colegio debe tener instalado y activado software antivirus autorizado. Los usuarios no deben desconectar el software antivirus. Todo usuario de los recursos informáticos tiene la responsabilidad de intentar evitar un caso de virus informático y su contagio. Nadie debe, a conciencia, crear, instalar, abrir o distribuir códigos maliciosos como virus o Trojan ni ningún otro programa destructivo.

4.14 Nadie debe a conciencia interferir con los mecanismos de seguridad o integridad de los recursos informáticos. Nadie debe usar los recursos informáticos para acceder a un uso no autorizado ni interferir con el uso legítimo de usuarios autorizados, de otros equipos en redes internas o externas. Se hará un seguimiento de accesos a redes.

4.15 De acuerdo con la legislación de protección de datos, Cognita o el colegio podría grabar o inspeccionar cualquier información transmitida por o contenida en sus equipos, incluyendo comunicaciones por email y sesiones de login, sin aviso previo en ciertas circunstancias que incluyen, pero no se limitan, a:

- Cuando existe duda razonable de que el usuario ha infringido esta política, consejos o procedimientos establecidos para proteger esta política;
- una cuenta parece tener actividad inusual o excesiva;
- hace falta proteger la integridad, seguridad o funcionalidad de los recursos informáticos o proteger a Cognita de responsabilidad legal;
- hay que establecer la existencia de hechos relevantes a la actividad de la empresa;
- hay que demostrar los estándares que deben alcanzar los usuarios de los equipos informáticos.
- Hay que buscar o recuperar mensajes perdidos debido a fallos técnicos;
- Para prevenir o detectar delito;
- Para investigar o detectar un uso no autorizado de los equipos informáticos;
- Para asegurar un uso efectivo de los recursos informáticos;
- Para determinar si las comunicaciones son relevantes a la actividad de la empresa (por ejemplo, en el caso de una baja o ausencia de un empleado y cuando la continuidad de la actividad de la empresa está en peligro); o
- Sea permitido o requerido por la ley.

4.16 El Equipo de Apoyo Técnico central, con el acuerdo del director, podría inspeccionar comunicaciones por e-mail o datos de usuarios por los motivos arriba mencionados. Otras comunicaciones basadas en Internet se monitorizan con software de forma automática.

4.17 Un sistema de CCTV hace un seguimiento de los exteriores del edificio 24 horas al día por motivos de seguridad y prevención de delito. Estos datos se graban.

No se debe mandar información privada, sensible o confidencial por mail no encriptado – sobre todo a un destinatario externo – ya que revelación accidental podría resultar en daño o incomodidad considerable. Se deben tratar datos personales de forma anónima cuando se pueda, por ejemplo, usando iniciales. Se debe usar contraseñas en documentos sensibles mandados a destinatarios externos. El Equipo de Apoyo Técnico puede aconsejar sobre soluciones de encriptación si se requiere.

4.18 No se debe crear páginas web en los equipos del colegio sin el permiso escrito del director.

4.19 Nadie puede usar los recursos informáticos para transmitir material abusivo, amenazante o acosador, cartas en cadena, spam, o comunicaciones prohibidas por ley o que podrían impactar de forma negativa sobre la imagen o reputación del colegio o Cognita. Nadie puede infringir las políticas de grupos, listas de correo u otros foros en los que participan a través de una cuenta del colegio.

4.20 Los usuarios deben cumplir los consejos de buena comunicación contenidos en la Política de Seguridad Digital.

4.21 En ningún momento está permitido descargar, crear ni acceder al siguiente contenido:

- Material pornográfico (contenido escrito, imágenes, grabaciones o video de una naturaleza sexual);
- material que de manera gratuita muestra imágenes de violencia, heridos o muerte;

- material que puede resultar en la vergüenza ajena:
- correo basura;
- material que promueve la intolerancia o discriminación por motivos de raza, género, discapacidad, orientación sexual, religión o edad;
- material relativo a la actividad criminal;
- música o video u otro material en incumplimiento de los derechos de autor;
- material que puede generar riesgos de seguridad o promover el mal uso de la informática.

4.22 Es posible que un usuario acceda a o sea dirigido a sitios web inaceptables por error. Puede ser difícil salir de estas páginas. Si un empelado ha accedido a contenido inaceptable o recibe material inaceptable por email, debe informar al director y/o al líder de salvaguarda. Podría evitar problemas más adelante si podemos alertar a los sistemas de seguimiento.

4.23 El director debe autorizar el acceso remoto a los sistemas del colegio y debe ser configurados por el Equipo Informático. Ejemplos de acceso remoto incluyen: webmail u otro sistema de email (Blackberry, Windows Mobile), email reenviado a una cuenta personal, conexión Virtual Private Network (VPN), Log Mein u otra conexión remota, portales web y herramientas de sincronización como Dropbox. Un empleado autorizado para acceso remoto debe cumplir con las condiciones de uso.

4.24 Los usuarios no deben conectar equipos personales a la red del colegio sin la autorización del director.

4.25 Todo equipo portátil se debe guardar de forma segura cuando no está en uso. Los empleados autorizados a llevarse equipos a casa o para *roaming* deben tomar las medidas razonables para mantener estos equipos a salvo.

4.26 Por motivos de seguridad los usuarios deben cerrar sesión o cerrar el ordenador si esperan estar fuera de su puesto durante un tiempo. Los usuarios deben apagar sus equipos al final de la jornada.

4.27 Los empleados no deben copiar ni instalar software del colegio en sus equipos personales sin autorización del director.

4.28 El personal tiene acceso a equipos digitales de grabación para usar como parte de sus clases. Como parte del currículo, se debe compartir con los alumnos el uso seguro y apropiado de equipos de grabación y referirse a ello cada vez que se haga una grabación.

4.29 Los empleados no deben usar imágenes ni grabaciones para actividades ajenas a proyectos autorizados por el colegio. No se debe distribuir material en el dominio público ni se debe usar para beneficio propio.

5. Comunicación por teléfono móvil y mensajería instantánea

5.1. Los empleados no deben comunicar su número de teléfono personal de casa o móvil a los estudiantes. El uso de teléfonos móviles personales no está permitido en la presencia de niñas, niños y adolescentes. **El colegio debe proporcionar dispositivos corporativos para visitas educativas.**

5.2. No se debe hacer fotos ni realizar grabaciones con un dispositivo móvil, incluidos los relojes inteligentes. Las fotos se deben hacer con un dispositivo propiedad del colegio, para uso aprobado del colegio y con el permiso del director.

5.3. El personal no debe usar los números de teléfono móvil de los estudiantes para hacer o recibir llamadas, o enviar o recibir mensajes al menos que sea durante una actividad autorizada del colegio.

5.4. Los empleados solo deben comunicarse de forma electrónica con los estudiantes desde cuentas de correo del colegio – por ejemplo, sobre trabajos o deberes.

5.5. Los empleados no deben realizar comunicaciones por mensaje con los estudiantes por una vía que no sea las cuentas y el sistema informático del colegio, y solo en el caso de actividad autorizada por el colegio.

5.6. Los empleados no deben contestar llamadas personales ni realizar mensajes personales cuando están trabajando.

6. Redes Sociales

6.1. Los empleados no deben comunicarse ni conectar con un estudiante o egresado menor de 18 años por una red social, sin el permiso escrito del director.

6.2. Los empleados no deben crear grupos en redes sociales que vincula directamente al colegio, Redcol o Cognita sin el permiso escrito del director.

6.3. Los empleados no deben usar redes sociales para comentar asuntos relacionados con el trabajo ni usar su puesto en el colegio o Redcol en beneficio de sus propios intereses.

Propiedad y Consulta	
Patrocinador del documento	Chief Information Officer
Consejo legal especializado	Arjun Majumdar, Solicitor - EMW Law LLP
Revisado agosto 2021	Regional Safeguarding Lead – Alison Barnett
Destinatarios	
Destinatarios	Todo el personal y voluntarios del colegio Todo el personal de la oficina regional/SCP.

Aplicación y Publicación del Documento	
Colombia	Si

Control versions	
Fecha implementación	Septiembre 2023
Fecha revisión	Revisión y actualización para implementación Agosto del 2023

Documentación relacionada	
Documentación relacionada	Todas las políticas de *Safeguarding* Código de Conducta Employee Handbook Keeping Children Safe in Education, as amended Working Together to Safeguard Children, as amended BSO Standards Política de Protección de Datos Data Protection Policy