Política de segurança eletrônica

1 **Âmbito de aplicação**

1.1 A Escola está empenhada em promover e salvaguardar o bem-estar de todos os alunos e uma estratégia de segurança online eficaz é fundamental para isso.

1.2 Os objetivos da estratégia de segurança online da Escola são três:

1. Proteger toda a comunidade escolar de conteúdo ou contacto ilegais, inadequados e prejudiciais;
2. Educar toda a comunidade escolar sobre o acesso e uso da tecnologia; e
3. Estabelecer mecanismos eficazes para identificar, intervir e escalar incidentes, quando apropriado.

1.3 Ao considerar o escopo da estratégia de segurança online da Escola, a Escola adotará uma abordagem ampla e intencional para considerar o que se enquadra no significado de tecnologia, redes e dispositivos usados para visualizar ou trocar informações, incluindo tecnologia de comunicação (coletivamente referidos nesta política como Tecnologia).

1.4 Esta política se aplica a todos os membros da comunidade escolar, incluindo funcionários e voluntários, alunos, pais e visitantes, que têm acesso à tecnologia da escola, dentro ou fora das instalações da escola, ou de outra forma usam a tecnologia de uma forma que afete o bem-estar de outros alunos ou de qualquer membro da comunidade escolar ou onde a cultura ou reputação da escola é colocada em risco.

1.5 As seguintes políticas, procedimentos e materiais de recursos também são relevantes para as práticas de segurança online da Escola:

Política Anti-Bullying

Código de Conduta do Pessoal

Política de Uso Aceitável para Estudantes Política de Proteção

1.6 Essas políticas, procedimentos e materiais de recursos estão disponíveis para a equipe

1.7 Esta é uma política de toda a escola

2 Funções e responsabilidades

2.1 **O Proprietário / ISP**

2.1.1 O titular tem a responsabilidade geral de salvaguardar

dentro da Escola, incluindo a abordagem da Escola para segurança online e

o uso da tecnologia dentro da Escola.

2.1.2 O proprietário é obrigado a garantir que todos aqueles com responsabilidades de liderança e gestão na Escola promovam ativamente o bem-estar dos alunos. A adoção desta política faz parte da resposta dos proprietários a este dever.

2.1.3 O proprietário realizará uma revisão anual dos procedimentos de salvaguarda da Escola e sua implementação, que incluirá a consideração da eficácia desta política e das políticas relacionadas no cumprimento dos objetivos estabelecidos no parágrafo 1.2 acima.

2.2 **Liderança Principal e Sênior e Equipe de Gestão**

2.2.1 O Diretor tem responsabilidade executiva geral pela segurança e bem-estar dos membros da comunidade escolar.

2.2.2 Os Líderes de Salvaguarda Designados (DSL) são membros seniores da equipe de Liderança Sênior e Gestão Escolar (SLMT) com responsabilidade principal pela salvaguarda e proteção infantil. A responsabilidade da DSL inclui gerenciar incidentes de proteção envolvendo o uso da Tecnologia da mesma forma que outros assuntos de proteção, de acordo com a Política de Salvaguarda da Escola.

2.2.3 Os DSLs trabalharão com o Chefe de TIC e o Gerente de TI (veja abaixo) no monitoramento dos usos e práticas da Tecnologia em toda a Escola e avaliando se alguma melhoria pode ser feita para garantir a segurança online e o bem-estar dos alunos.

2.2.4 As DSLs monitorarão regularmente o Registro de Incidentes de Tecnologia mantido pelo Gerente de TI.

2.2.5 A DSL atualizará regularmente outros membros da SLMT sobre a operação dos acordos de salvaguarda da Escola, incluindo práticas de segurança online.

2.3 **Gerente de TI**

2.3.1 O Gestor de TI, juntamente com a sua equipa, é responsável pelo funcionamento eficaz do sistema de filtragem da Escola, de modo a que os alunos e o pessoal não possam aceder a qualquer material que represente um risco de salvaguarda, incluindo material terrorista e extremista, durante a utilização da rede da Escola.

2.3.2 O Gerente de TI é responsável por garantir que:

(a) a infraestrutura de tecnologia da Escola é segura e, na medida do possível, não está aberta a uso indevido ou ataque malicioso;

(b) o usuário só pode usar a Tecnologia da Escola se estiver devidamente autenticado e autorizado;

(c) a Escola tem uma política de filtragem eficaz em vigor e que é aplicada e atualizada regularmente;

(d) os riscos de estudantes e pessoal contornarem as salvaguardas estabelecidas pela Escola sejam minimizados;

(e) o uso da Tecnologia da Escola é monitorado regularmente para garantir a conformidade com esta política e que qualquer uso indevido ou tentativa de uso indevido pode ser identificado e relatado à pessoa apropriada para investigação; e

(f) o software e os sistemas de monitoramento são mantidos atualizados para permitir que a equipe de TIC monitore o uso de e-mail e da Internet na rede da Escola e mantenha registros de tal uso.

2.3.3 O gestor informático fornecerá pormenores, mediante pedido, descrevendo a actual disposição técnica e as salvaguardas em vigor para filtrar e monitorizar conteúdos inadequados e alertar a Escola para questões de salvaguarda.

2.3.4 O Gerente de TI informará regularmente ao SLMT sobre a operação da Tecnologia da Escola. Se o Gerente de TI tiver dúvidas sobre a funcionalidade, eficácia, adequação ou uso da Tecnologia dentro da Escola, ele encaminhará essas preocupações prontamente para o(s) membro(s) apropriado(s) da Equipe de Liderança Sênior da Escola (SL T).

2.3.5 O Gerente de TI é responsável por manter o Registro de Incidentes de Tecnologia e levar quaisquer questões de preocupação de salvaguarda à atenção da DSL de acordo com a Política e Procedimentos de Proteção e Proteção à Criança da Escola.

2.4 **Todos os funcionários**

2.4.1 Os funcionários da Escola têm a responsabilidade de agir como um bom modelo no uso da Tecnologia e de compartilhar seus conhecimentos sobre as políticas da Escola e sobre práticas seguras com os alunos.

2.4.2 Espera-se que o pessoal cumpra, na medida do aplicável, cada uma das políticas referidas no ponto 1.5 acima.

2.4.3 Os funcionários têm a responsabilidade de relatar quaisquer preocupações sobre o bem-estar e a segurança de um aluno de acordo com esta política e a Política de Salvaguarda e Proteção à Criança da Escola.

2.5 **Pais**

2.5.1 O papel dos pais em garantir que os alunos entendam como se manter seguros ao usar a tecnologia é crucial. A Escola espera que os pais promovam práticas seguras ao usar a Tecnologia e que:

(a) apoiar a Escola na implementação desta política e relatar quaisquer preocupações de acordo com as políticas e procedimentos da Escola;

(b) conversar com seus filhos para entender as maneiras pelas quais eles estão usando a Internet, as mídias sociais e seus dispositivos móveis e promover um comportamento responsável; e

(c) incentivar seu filho a falar com alguém se estiver sofrendo bullying ou estiver preocupado com sua própria segurança ou a de outro aluno ou precisar de apoio.

2.5.2 Se os pais tiverem alguma dúvida ou precisarem de qualquer informação sobre segurança online, eles devem entrar em contato com a DSL.

Educação e formação

3.1 **Alunos**

3.1.1 O uso seguro da tecnologia é parte integrante do currículo de TIC da Escola. Os alunos são educados de maneira apropriada à idade sobre a importância do uso seguro e responsável da tecnologia, incluindo a internet, mídias sociais e dispositivos eletrônicos móveis (consulte a Política Curricular da Escola).

3.1.2 A tecnologia está incluída nos programas educativos seguidos no Ano Europeu das Pescas das seguintes formas:

(a) as crianças são orientadas a dar sentido ao seu mundo físico e à sua comunidade por meio de oportunidades para explorar, observar e descobrir pessoas, lugares, tecnologia e meio ambiente;

(b) as crianças podem explorar e brincar com uma ampla variedade de mídias e materiais e têm oportunidades e incentivo para compartilhar seus pensamentos, ideias e sentimentos por meio de uma variedade de atividades em arte, música, movimento, dança, dramatização, design e tecnologia; e

(c) as crianças são orientadas a reconhecer que uma variedade de tecnologias é usada em locais como residências e escolas e incentivadas a selecionar e usar a tecnologia para fins específicos.

3.1.3 O uso seguro da tecnologia também é um foco em todas as áreas do currículo e as principais mensagens de segurança são reforçadas como parte das assembleias e atividades tutoriais/pastorais, ensinando os alunos

1. (a) sobre os riscos associados ao uso da Tecnologia e como proteger a si mesmos e seus pares de riscos potenciais;
2. (b) estar criticamente ciente do conteúdo que acessam online e ser guiado para validar a precisão das informações;
3. c) Como reconhecer comportamentos suspeitos, intimidadores, de radicalização e extremistas;
4. d) A definição de ciberassédio, os seus efeitos na vítima e a forma de tratar cada um deles.

   identidades online de outras pessoas com respeito;

5. (e) as consequências do comportamento negativo online; e
6. (f) como denunciar cyberbullying e/ou incidentes que fazem os alunos se sentirem

desconfortável ou sob ameaça e como a Escola lidará com aqueles que se comportam mal. A Política de Uso Aceitável de TIC da Escola para Alunos estabelece as regras da Escola sobre

3.1.4 O uso da Tecnologia, incluindo internet, e-mail, mídia social e dispositivos eletrônicos móveis, ajudando os alunos a proteger a si mesmos e aos outros ao usar a Tecnologia. Os alunos são lembrados da importância desta política regularmente.

3.2 **Funcionários**

3.2.1 A Escola oferece treinamento sobre o uso seguro da Tecnologia aos funcionários, para que eles estejam cientes de como proteger os alunos e a si mesmos dos riscos do uso da Tecnologia e lidar adequadamente com incidentes envolvendo o uso da Tecnologia quando eles ocorrerem.

3.2.2 O treinamento de indução para novos funcionários inclui orientação sobre esta política, bem como o Código de Conduta da Equipe, a Política de E-mail e Internet e a Política de Diretrizes de Uso Profissional de Mídias Sociais. O treinamento contínuo de desenvolvimento de pessoal inclui treinamento em segurança tecnológica, juntamente com questões específicas de proteção, incluindo cyberbullying e radicalização.

3.2.3 Os funcionários também recebem orientações sobre protecção de dados na indução e a intervalos regulares posteriormente.

3.2.4 A frequência, o nível e a orientação desta formação dependerão das funções e necessidades individuais e serão fornecidos como parte da abordagem global da Escola em matéria de salvaguarda.

3.3 **Pais**

3.3.1 As informações estão disponíveis para os pais através do portal Firefly. Além disso, oferecemos aos pais a oportunidade de participar de sessões escolares sobre segurança online anualmente.

3.3.2 Os pais são incentivados a ler a Política de Uso Aceitável para Alunos com seu filho/filha para garantir que ela seja totalmente compreendida.

3.4 **Recursos úteis**

3.4.1 Existem recursos úteis sobre o uso seguro da tecnologia disponíveis por meio de vários

Sites, incluindo:

a) http://www.thinkuknow.co.uk/

b) https://www.disrespectnobody.co.uk/

c) http://www.saferinternet.org.uk/

d) https://www.internetmatters.org/

e) http://educateagainsthate.com/

f) http://www.kidsmart.org.uk/

g) http://www.safetynetkids.org.uk/

h) http://www.safekids.com/

i) http://parentinfo.org/

4 **Acesso à tecnologia da escola**

4.1 A Escola fornece acesso à Internet e intranet e um sistema de e-mail para alunos e funcionários, bem como outras tecnologias. Alunos e funcionários devem cumprir a respectiva Política de Uso Aceitável de Tecnologia ao usar a Tecnologia Escolar. Todo esse uso é monitorado pelo Gerente de TI e sua equipe.

4.2 Os alunos e funcionários precisam de nomes de usuário e senhas individuais para acessar os sites da Internet e intranet da Escola e o sistema de e-mail, que não devem ser divulgados a nenhuma outra pessoa. Qualquer aluno ou membro da equipe que tenha um problema com seus nomes de usuário ou senhas deve denunciá-lo ao Departamento de TI imediatamente.

4.3 Nenhum laptop, tablet ou outro dispositivo eletrônico móvel pode ser conectado à rede da Escola sem o consentimento do Gerente de TI. Todos os dispositivos conectados à rede da escola devem ter um software antivírus atual e atualizado instalado e ter as atualizações mais recentes do sistema operacional aplicadas. O uso de qualquer dispositivo conectado à rede da Escola será registrado e monitorado pelo Departamento de Suporte de TI.

4.4 A Escola tem uma conexão Wi-Fi separada disponível para uso pelos visitantes da Escola. Uma senha, que é alterada regularmente, deve ser obtida com um membro da equipe para usar o Wi-Fi. O uso deste serviço será registrado e monitorado pelo Departamento de TI.

4.5 **Uso de dispositivos eletrônicos móveis**

4.5.1 A Escola possui sistemas apropriados de filtragem e monitoramento para proteger os alunos que usam a Internet (incluindo e-mail, mensagens de texto e sites de mídia social) quando conectados à rede da Escola. Os dispositivos móveis equipados com uma assinatura de dados móveis podem, no entanto, fornecer aos alunos acesso ilimitado e irrestrito à Internet. Como a Escola não pode oferecer proteção adequada para os alunos, os alunos não têm permissão para usar seus dispositivos móveis para se conectar à Internet, incluindo o acesso a e-mail, mensagens de texto ou sites de mídia social quando estiverem sob os cuidados da Escola. Em certas circunstâncias, um aluno pode receber permissão para usar seu próprio dispositivo móvel para se conectar à Internet usando a rede da Escola. A permissão para fazê-lo deve ser solicitada e dada com antecedência.

4.5.2 As regras da Escola sobre o uso de dispositivos eletrônicos móveis estão estabelecidas na Política de Uso Aceitável de Tecnologia para Alunos.

4.5.3 A utilização de dispositivos eletrónicos móveis pelo pessoal é abrangida pelo Código de Conduta do pessoal. Salvo acordo em contrário por escrito, dispositivos móveis pessoais, incluindo laptops e notebooks, não devem ser usados para fins escolares, exceto em caso de emergência.

4.5.4 As políticas da Escola se aplicam ao uso da Tecnologia por funcionários e alunos, dentro ou fora das instalações da Escola, e as medidas apropriadas serão tomadas quando tal uso afetar o bem-estar de outros alunos ou de qualquer membro da comunidade escolar ou quando a cultura ou reputação da Escola for colocada em risco.

5 **Procedimentos para lidar com incidentes de uso indevido**

5.1 Funcionários, alunos e pais são obrigados a relatar incidentes de uso indevido ou suspeita de uso indevido à Escola de acordo com esta política e as políticas e procedimentos disciplinares e de salvaguarda da Escola.

5.2 **Uso indevido por alunos**

5.2.1 Qualquer pessoa que tenha alguma preocupação com o uso indevido da Tecnologia por parte dos alunos deve denunciá-la para que possa ser tratada de acordo com as políticas de comportamento e disciplina da Escola, incluindo a Política Anti-Bullying onde houver uma alegação de cyberbullying.

5.2.2 Qualquer pessoa que tenha alguma preocupação com o bem-estar e a segurança de um aluno deve denunciá-la imediatamente, de acordo com os procedimentos de proteção infantil da Escola (consulte a Política de Salvaguarda e Proteção à Criança da Escola.

5.3 **Uso indevido pela equipe**

5.3.1 Qualquer pessoa que tenha alguma preocupação com o uso indevido da Tecnologia por parte dos funcionários deve denunciá-la de acordo com a Política de Denúncias da Escola para que possa ser tratada de acordo com os procedimentos disciplinares da equipe.

5.3.2 Se alguém tiver uma preocupação relacionada à salvaguarda, deve denunciá-la imediatamente para que possa ser tratada de acordo com os procedimentos para denunciar e lidar com alegações de abuso contra funcionários estabelecidos na Política de Salvaguarda e Proteção à Criança da Escola.

5.4 **Uso indevido por qualquer usuário**

5.4.1 Qualquer pessoa que tenha uma preocupação com o uso indevido da Tecnologia por qualquer outro usuário deve denunciá-la imediatamente ao Chefe de TIC ou ao Diretor.

5.4.2 A Escola reserva-se o direito de retirar o acesso à rede da Escola por qualquer usuário a qualquer momento e de denunciar suspeitas de atividades ilegais à polícia.

6 **Monitoramento e revisão**

6.1 Todos os incidentes graves envolvendo o uso da Tecnologia serão registrados centralmente no Registro de Incidentes de Tecnologia pelo Gerente de TI.

6.2 A DSL é responsável pela implementação e revisão desta política e considerará o registro de incidentes envolvendo o uso da Tecnologia e os registros de atividades na Internet (incluindo sites visitados) como parte do monitoramento contínuo dos procedimentos de salvaguarda, para considerar se as práticas de segurança e proteção online existentes na Escola são adequadas.

A consideração da eficácia dos procedimentos de segurança online da Escola e a educação dos alunos sobre como se manter seguro online serão incluídas na revisão anual de salvaguarda dos Governadores.