



**PROGRESSO  
BILÍNGUE**



## **Política de segurança eletrônica/E Safety - 2025**

**1.1** O **Colégio Progresso Bilíngue Itu** está empenhado 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:

- Proteger toda a comunidade escolar de conteúdos ou contatos ilegais, inadequados e prejudiciais;
- Educar toda a comunidade escolar sobre o acesso e uso da tecnologia;
- Estabelecer mecanismos eficazes para identificar, intervir e escalar incidentes, quando apropriado.

**1.3** Ao considerar o escopo da estratégia de segurança online do **Colégio Progresso Bilíngue Itu**, 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 seja 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 para segurança online e o uso da tecnologia dentro da instituição.

**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.

**2.1.4** A Escola cumpre a legislação brasileira aplicável, incluindo a Lei nº 12.965/2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, reforçando a importância da segurança e proteção online no ambiente escolar.

## **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 atual 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 (SLT).

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) apoiem a Escola na implementação desta política e relatem quaisquer preocupações de acordo com as políticas e procedimentos da Escola;
- (b) conversem com seus filhos para entender as maneiras pelas quais eles estão usando a Internet, as mídias sociais e seus dispositivos móveis, promovendo um comportamento responsável; e
- (c) incentivem seu filho a falar com alguém caso esteja sofrendo bullying, preocupado com sua própria segurança ou a de outro aluno, ou precise de apoio.

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

## **3. 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 internet, mídias sociais e dispositivos eletrônicos móveis (conforme a Política Curricular da Escola).

3.1.2 A tecnologia está incluída nos programas educativos do Ano Escolar 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, sendo incentivadas a compartilhar seus pensamentos, ideias e sentimentos por meio de atividades em arte, música, movimento, dança, dramatização, design e tecnologia;
- (c) as crianças são orientadas a reconhecer que diversas tecnologias são usadas em locais como residências e escolas, sendo incentivadas a selecionar e usar a tecnologia para fins específicos.

3.1.3 O uso seguro da tecnologia é foco em todas as áreas do currículo, com as principais mensagens de segurança reforçadas em rodas de conversa nas salas de aula, comunicados e atividades/palestras oferecidas para pais e alunos, anualmente, ensinando os alunos:

- (a) sobre os riscos associados ao uso da Tecnologia e como proteger a si mesmos e seus pares de potenciais riscos;
- (b) a estar criticamente conscientes do conteúdo acessado online e a validar a precisão das informações;
- (c) a reconhecer comportamentos suspeitos, intimidadores, de radicalização e extremistas;
- (d) a entender a definição de ciberassédio, seus efeitos na vítima e como lidar com cada situação;
- (e) a tratar as identidades online de outras pessoas com respeito;
- (f) as consequências do comportamento negativo online;

(g) como denunciar cyberbullying e/ou incidentes que causem desconforto ou ameaça, bem como como a Escola lidará com os responsáveis por comportamentos inadequados. A Política de Uso Aceitável de TIC para Alunos estabelece as regras da Escola sobre estes temas.

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

### **3.2 Funcionários**

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

3.2.2 O treinamento de indução para novos funcionários inclui orientação sobre esta política, 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 desenvolvimento contínuo inclui formação em segurança tecnológica, abordando também questões específicas de proteção, como cyberbullying e radicalização.

3.2.3 Os funcionários recebem orientações sobre proteção de dados na indução e em intervalos regulares posteriormente.

3.2.4 A frequência, o nível e o conteúdo da formação dependem das funções e necessidades individuais e fazem parte da abordagem global da Escola em matéria de salvaguarda.

### **3.3 Pais**

3.3.1 As informações para pais estão disponíveis por meio do aplicativo Agenda Edu e site do colégio. Além disso, a Escola oferece oportunidades anuais para participação dos pais em palestras sobre segurança online.

3.3.2 Os pais são incentivados a ler a Política com seus filhos, garantindo plena compreensão.

### **3.4 Recursos úteis**

3.4.1 Existem diversos recursos disponíveis sobre uso seguro da tecnologia, 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, intranet e sistema de e-mail para alunos e funcionários, bem como outras tecnologias. O uso da Tecnologia Escolar deve respeitar a respectiva Política de Uso Aceitável. Todo o uso é monitorado pelo Gerente de TI e sua equipe.

4.2 Alunos e funcionários precisam de nomes de usuário e senhas individuais para acessar os sistemas da Escola, que não devem ser compartilhados. Problemas com acesso devem ser imediatamente comunicados ao Departamento de TI.

4.3 Nenhum laptop, tablet ou dispositivo eletrônico móvel pode ser conectado à rede da Escola sem consentimento do Gerente de TI. Todos os dispositivos conectados devem ter antivírus atualizado e as últimas atualizações do sistema operacional instaladas. O uso destes dispositivos será registrado e monitorado pelo Departamento de TI.

4.4 A Escola disponibiliza conexão Wi-Fi separada para visitantes, com senha alterada regularmente, disponível mediante solicitação a um membro da equipe. O uso do Wi-Fi será registrado e monitorado pelo Departamento de TI.

#### **4.5 Uso de dispositivos eletrônicos móveis**

4.5.1 A Escola possui sistemas adequados de filtragem e monitoramento para proteger os alunos ao usarem a Internet (incluindo e-mail, mensagens e redes sociais) conectados à rede da Escola. Dispositivos móveis com assinatura de dados móveis podem dar acesso irrestrito à Internet, o que não pode ser adequadamente protegido pela Escola. Por isso, alunos não podem usar seus dispositivos móveis para acessar a Internet (incluindo e-mail, mensagens ou redes sociais) enquanto estiverem sob cuidados da Escola. Em certas circunstâncias, o uso do dispositivo móvel pessoal na rede da Escola pode ser autorizado mediante prévia solicitação e aprovação.

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

4.5.3 O uso de dispositivos móveis por funcionários é regido pelo Código de Conduta do pessoal. Exceto em emergências, dispositivos pessoais, incluindo laptops e notebooks, não devem ser usados para fins escolares sem autorização.

4.5.4 As políticas da Escola aplicam-se ao uso da Tecnologia por funcionários e alunos, dentro ou fora da Escola, e medidas apropriadas serão tomadas se o uso afetar o bem-estar de outros ou colocar em risco a cultura ou reputação da Escola.

#### **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.