Programa Proteja-se dos Prejuízos do Cyberbullying

Código de Conduta Digital para Educadores

SLM

SIQUEIRA LAZZARESCHI DE MESQUITA

ADVOGADOS

COLÉGIO PIAGET

INFANTIL • FUNDAMENTAL • MÉDIO

SLM

SIQUEIRA LAZZARESCHI DE MESQUITA

ADVOGADOS

SUMÁRIO

SLM

SIQUEIRA LAZZARESCHI DE MESQUITA

ADVOGADOS

SOBRE O PROGRAMA DE COMBATE AO BULLYING DO COLÉGIO PIAGET SBC

EXPOSIÇÃO SOBRE O SURGIMENTO E DESENVOLVIMENTO DO PROGRAMA E O CONTEXTO ATUAL E OS NOVOS PROBLEMAS NO AMBIENTE ESCOLAR PRIVADO E PUBLICO

O programa surgiu em decorrência da A Lei nº 13.185/15 que tornou obrigatória a implantação do Programa de Combate à Intimidação Sistemática (bullying) em todas as instituições de ensino, clubes e agremiações recreativas. A lei entrou em vigor em fevereiro de 2016, em razão do aumento dos processos judiciais derivados da violência sistemática entre alunos e pais, principalmente nos grupos de WhatsApp e redes sociais.

O cyberbullying combate-se com educação, informação e conhecimento das regras que regem o relacionamento virtual nas redes sociais. Portanto, é necessário que a equipe pedagógica, pais e alunos tenham conhecimento sobre as consequências legais que os incidentes digitais ocasionam.

No intuito de auxiliar as escolas no trabalho de educação digital, a advogada Dra. Ana Paula Siqueira Lazzareschi de Mesquita desenvolveu o programa educacional "Proteja-se dos Prejuízos do Cyberbullying" em maio de 2014, utilizando-se de linguagem jurídica-pedagógica para dialogar com pais, alunos e professores, sem pedantismo e com termos compreensíveis para todas as idades e classes sociais.
O programa é desenvolvido dentro da linguagem e filosofia pedagógica institucional, propiciando aos diretores, coordenadores, orientadores e mantenedores suporte jurídico-pedagógico para a prevenção, combate e diagnose da violência sistemática.
Atualmente, com o aumento do acesso a internet, os problemas com cyberbullying aumentam consideravelmente! Temos além de ofensas entre alunos, pais e professores e disseminação de desafios e brincadeiras perigosas e as famosas fake News que podem causar danos irreversíveis na vida das pessoas.
Toda essa problemática exige uma ação efetiva e séria e para isso o programa se torna essencial.

A conscientização e a prevenção, ainda que nessa área, ainda são a melhor forma de se evitar incidentes digitais e presenciais.

SLM

SIQUEIRA LAZZARESCHI DE MESQUITA

ADVOGADOS

APRESENTAÇÃO DO QUE O PROBLEMA CONSTATOU, COMO ATUOU PARA ESTIMULAR AS ESCOLAS A ENFRENTAR O PROBLEMA, RESULTADOS MENSURADOS.

Os danos psicológicos, morais e físicos causados pelo bullying presencial e digital crescem no Brasil de forma exponencial, causando justa preocupação nos educadores, famílias e autoridades públicas.
Para que o Programa "Proteja-se dos Prejuízos do Cyberbullying" seja realmente eficaz é necessário o envolvimento da comunidade escolar do Colégio Piaget com o tema. Afinal, o cyberbullying é o ápice da ausência de educação digital, sendo certo que é papel da instituição de ensino oferecer informação e material de consulta idôneo para a prevenção de incidentes virtuais.

Não basta apenas falar de bullying – é necessário que docentes e discentes saibam as consequências (jurídicas, pedagógicas e sociais), diretas e indiretas de comportamentos que visam a ofensa, humilhação ou exclusão das vítimas, que frequentemente ocorrem nos malfadados grupos de WhatsApp de alunos ou de mães.

Docentes, pais e alunos precisam ter em mente que os atos que Bullying, racismo, injúria racial, instigação ao suicídio, ameaça, lesão corporal e as ofensas contra a honra (calúnia, difamação e injúria) são crimes e os autores estão sujeitos às penas previstas em lei.

A orientação jurídica-pedagógica correta inibe e previne a ação violenta em grupos de WhatsApp e redes sociais. Quando a escola fornece o curso de capacitação de docentes, nos termos do inciso II do Artigo 4º da Lei do Bullying, os educadores estarão aptos a diagnosticar e intervir precocemente nos casos de violência sistemática.

OBJETIVOS DO PROGRAMA DE COMBATE AO BULLYING

- Instituir e complementar o programa de combate ao bullying de acordo com a metodologia pedagógica do colégio e com todos os requisitos da Lei 13.185/15 e artigo 12 da LDB
- Conscientizar a comunidade escolar sobre consequências sociais e jurídicas do cyberbullying
- Apresentar ações de prevenção, diagnose e combate ao bullying e cyberbullying
- Criar sólidas políticas de compliance escolar
- Criar canais especificos para o atendimento aos colaboradores da escola, familias e alunos.

- Auxiliar a comunicação e elaboração de documentos e registro nos órgãos públicos competentes, nos termos da Lei nº 13.185/15 e LDB

COLÉGIO PIAGET PERANTE A INOVAÇÃO TECNOLOGICA E CIENTÍFICA

O Colégio Piaget tem como objetivo desenvolver a capacidade criativa do valor, a sensibilidade e a intuição nas crianças. Cultivar o caráter criativo do valor fazendo resplandecer a inteligência criativa do interior de cada indivíduo – eis a força universal pela qual todas as pessoas se capacitarão a realizar a felicidade, transcendendo o tempo e o espaço.

Seguindo esse princípio básico, o Colégio Piaget apoia e incentiva a participação nos movimentos de produção intelectual, científica e tecnológica que venham a melhorar a vida das pessoas. O ponto-chave da educação para a paz é erradicar o preconceito e a discriminação do coração das pessoas. No Colégio Piaget, a coordenação pedagógica decidiu pela política de aprofundamento da compreensão mútua entre os grupos sociais, ou seja, não só promover a compreensão, mas também desenvolver o respeito a essas diferenças.

O desafio agora é usufruir os benefícios da Comunicação Digital dentro dos princípios morais e éticos da convivência social.

O Colégio Piaget diariamente se esforça para proporcionar atividades que ajudem as crianças a compreender a importância de fazer os outros felizes aplicando o que aprenderam em sala de aula e acredita que essa é a característica fundamental da educação humanística.

A cartilha visa orientar o uso dessa tecnologia de forma ética e benéfica. É importante que cuidados sejam tomados para que a participação nas redes sociais, sites, blogs e aplicativos seja algo proveitoso e útil na construção de valores humanos. Seguem alguns exemplos de prevenção a incidentes digitais feitos pelo Colégio Piaget:

- Criação de código de conduta digital;

- Informação aos funcionários e professores sobre as regras de acesso durante o expediente e sobre o comportamento esperado, referente a divulgação de informações profissionais (confidenciais ou não) e a emissão de opiniões que possam comprometer o colégio;

- Campanhas periódicas de conscientização para os funcionários, professores, pais e alunos, informando-os sobre os riscos de uso das redes sociais e aplicativos de celulares;

- Investimento em treinamento, principalmente para os funcionários responsáveis pelo perfil @colegiopiagetsbc e dos professores;

- Observação quanto à opinião de pais, alunos e professores ou qualquer ação que envolva o nome Colégio Piaget do Brasil, para que seja capaz de tomar atitudes em tempo de evitar algum dano à imagem.

OBS: Na tabela da página 04 acrescentar mais uma lei: Lei do *Bullying* – Lei n.° 13.185/2015.

2. O PROFESSOR DA ERA DIGITAL

2.1 Professores, pais e alunos

A comunicação efetiva entre esses três elementos é essencial para o sucesso ou fracasso na implantação de um programa de uso de comunicação digital sadio e agradável.

Espera-se que da interação professor-alunos-pais resultem na prevenção de eventos digitais indesejados e a identificação de fatos reais que necessitem da atuação da direção escolar.

Ao educador cabe transmitir aos alunos e pais de forma clara e explícita as consequências legais do uso indevido da Internet e aplicativos de celulares.

Não é escopo do educador atuar como técnico de informática, psicólogo ou advogado. Para tanto deverão ser consultados os especialistas de cada área.

2.1.2 Comunicação

O professor e o aluno serão os representantes da Colégio Piaget neste processo, sendo que os preceitos e normas de comportamento social são aqueles contemplados na filosofia de ensino do Colégio, cuja adesão foi feita pelos responsáveis por ocasião da matrícula.

O professor do Colégio Piaget representa a Instituição na intervenção com os alunos, sendo o principal elo de pacificação social escolar.

Para iniciarmos este manual, comecemos com o seguinte questionamento: Você realmente conhece os seus filhos e alunos? Tem certeza? Ok, vamos fazer um "tira-teima"...

a) Quantos alunos possuem perfis em redes sociais e são menores de 13 anos?
b) Você compartilha seu perfil e interage com pais e alunos em redes sociais?
c) Você sabe se o aluno copiou da Internet o trabalho solicitado?
d) Você utiliza WhatsApp, Telegram?
f) Você sabe o que é *sexting*?
g) Seus alunos mandam mensagens pelo celular durante as aulas ou provas ou intervalos?

Se você respondeu "não" para a maioria das perguntas... não tem problema. Esse manual ajudará a esclarecer essas questões.

Agora você deve estar pensando: "Nossa, como é difícil ser professor hoje em dia!". Sim, é verdade. Não é fácil ser professor na ERA DIGITAL. Mas alguns conceitos e dicas podem ajudar muito a dinâmica na sala de aula, melhorando o aprendizado e a qualidade de vida de todos.

Vamos lá?!

3 SEJA BEM-VINDO AO DESCONHECIDO MUNDO DIGITAL

O mundo digital é um universo desconhecido, mesmo para as pessoas que utilizam a Internet todos os dias. Saber navegar na web é uma coisa. Mas conhecer como ela realmente funciona e seus reais perigos, quase ninguém sabe! Por isso, seja bem-vindo ao desconhecido mundo digital!

Solicitamos que estejam atentos em relação aos termos de uso e política de privacidade de sites, redes sociais e aplicativos de celulares.

Muito cuidado ao indicar sites de pesquisa para os alunos, antes de passar para os discentes, o professor Piaget lê, COM MUITA ATENÇÃO, a política de uso do site, que será objeto da pesquisa. Atenção em relação à indicação de faixa etária!

3.1 Defina: Rede Social

É uma estrutura social composta por pessoas, empresas, associações, entre outros, que compartilham valores (afetivos, sociais, religiosos etc) ou objetivos comuns, sendo que a principal conexão entre os participantes é a própria identidade.

3.1.2 Quais os riscos? O que pode ser feito como prevenção?

1° Grande quantidade de usuários: Considere que você está em um local público, de grande visibilidade, mais perigoso que a rua.

Seja cuidadoso ao se associar a grupos e comunidades, como professor, você tem uma imagem pessoal e corporativa que deve ser preservada. Cuidado com comunidades que divulguem a discriminação de raça, credo, condição social, opção sexual ou que incentivem.

Disputas públicas com outros docentes sobre posições religiosas e políticas devem ser evitadas, principalmente se alunos estão observando as postagens feitas.

2° Grande quantidade de informações pessoais disponíveis para consulta: Mantenha seu perfil e seus dados privados, essa pode ser uma porta aberta para o envio de vírus, SPAM ou conteúdo impróprio.

Restrinja o acesso ao seu endereço de e-mail pessoal e seja seletivo ao aceitar seus contatos, se você forneceu os dados para a comunicação para os amigos da rede social, posteriormente não poderá reclamar que as pessoas tentem entrar em contato com você.

3° Dificuldade de exclusão e controle de informações: Antes de divulgar uma informação, avalie se, de alguma forma, ela pode atrapalhar a sua carreira e não se esqueça jamais que pessoas do ambiente profissional podem ter acesso às postagens feitas.

Cuide da sua imagem profissional. Recomenda-se não aceitar alunos e responsáveis legais como amigos nas redes sociais, principalmente menores de 14 anos.

Evite a divulgação de conversas privadas, especialmente se essas ocorreram na sala dos professores.

Seja cuidadoso ao fornecer sua localização ou a divulgação de seus locais favoritos ou de frequência habitual. Leve sempre em conta:

- Tempo que as informações ficam disponíveis até a remoção de conteúdo impróprio;
- Facilidade de acesso e velocidade de propagação de informações (falsas e verdadeiras).

SLM

SIQUEIRA LAZZARESCHI DE MESQUITA

ADVOGADOS

Não acredite em tudo que está escrito ou publicado nas redes socais ou nos grupos de comunicação instatânea. Imagens podem ser adulteradas, inverdades podem ser ditas e palavras podem ser facilmente atribuídas a terceiros com muita facilidade.

DICAS DE USO

Pense bem antes de publicar informações pessoais, evitando registrar ou publicar fotos íntimas, com pouca roupa ou que possam te causar vergonha caso todos tenham acesso. Uma vez na rede, é quase impossível controlar e deletar essas imagens;

Cuidado ao adicionar pessoas desconhecidas ou menores de 14 anos como amigos. Nem sempre quem está do outro lado da tela é mesmo quem diz ser. Seguem dicas objetivas para seu dia a dia:

1. Senhas fortes:

- Crie senhas longas e complexas, utilizando letras maiúsculas, minúsculas, números e caracteres especiais. Ex: CamiLav@sques14!

- Evite usar informações pessoais óbvias, como datas de nascimento ou nomes de familiares/pets.

- Nunca compartilhe suas senhas com colegas ou amigos (em nenhuma hipótese).

2. Atualizações de software e aplicativos

- Mantenha seu sistema operacional, navegadores e aplicativos sempre atualizados para proteger contra vulnerabilidades conhecidas.

3. Phishing e golpes:

- Desconfie de e-mails, mensagens ou links suspeitos que solicitem informações pessoais ou financeiras.

- Não clique em links desconhecidos e não baixe arquivos de fontes não confiáveis.

4. Privacidade e redes sociais:

- Ajuste as configurações de privacidade das suas redes sociais para controlar quem pode ver suas informações pessoais e postagens.

- Evite compartilhar detalhes pessoais como endereço, telefone e informações da escola em redes públicas.

5. Comportamento online responsável:

- Seja respeitoso com os outros online.

6. Uso seguro de dispositivos:

- Ao usar computadores da escola ou dispositivos públicos, não salve informações pessoais e faça logout após o uso.

- Use antivírus sempre, autenticação em 2 fatores e mantenha os dispositivos protegidos contra malware.

7. Backup de dados:

- Faça backup regularmente (todos os dias preferencialmente) de seus trabalhos e arquivos importantes em um local seguro para evitar perda de dados em caso de incidentes.

8. Educação contínua sobre segurança digital:

- Esteja sempre atualizado sobre novas ameaças e práticas seguras através de workshops, palestras ou recursos online.

- Tenha um contato de emergência no seu celular (deve ser uma pessoa maior de 18 anos).

- Discuta com sua família sobre suas atividades online e solicite orientação da escola caso se sinta agredido ou ofendido.

9. Reporte de incidentes:

- Informe imediatamente ao Colegio Piaget caso você seja vítima de cyberbullying, assédio online ou qualquer forma de crime digital.

10. Uso ético e legal da tecnologia:

Políticas de uso aceitável: antes de utilizar qualquer plataforma digital, como redes sociais, sites ou aplicativos, leia as políticas de uso aceitável. Essas políticas definem o que é permitido na plataforma, incluindo restrições de publicação e compartilhamento de conteúdo.

Tenha cuidado com compartilhamento de conteúdos sensíveis: não compartilhe informações privadas, sensíveis ou protegidas por sigilo (como dados pessoais ou segredos comerciais, especialmente informações relativas aos alunos e/ou suas famílias) sem consentimento, respeitando leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

Utilize fontes confiáveis: ao coletar informações online, opte por fontes confiáveis e reconhecidas (sempre utilize o Google Academico). Favor não disseminar fake news ou conteúdos de procedência duvidosa, o que pode acarretar responsabilidade legal, especialmente se houver danos a terceiros. Se tiver dúvida da veracidade da notícia, buscar em https://www.cnj.jus.br/programas-e-acoes/painel-de-checagem-de-fake-news/ ou https://www.aosfatos.org/

Atente-se às regras de *fair use*: em alguns casos, como em pesquisas, críticas, comentários e paródias, o uso de obras protegidas pode ser permitido sob a doutrina de Fair Use. No entanto, essas exceções são limitadas e devem ser usadas com cuidado, sempre avaliando se o uso é realmente justo e necessário.Lembre-se: a segurança digital é essencial para proteger sua privacidade, seus dados pessoais e manter um ambiente online seguro e saudável para todos na escola.

REDES SOCIAIS E APLICATIVOS

- EXIGÊNCIA DE IDADE MÍNIMA

Os professores e colaboradores estarão sempre atentos aos termos de uso e política de privacidade de sites, redes sociais e aplicativos de celulares.

Exemplos:

Facebook / Instagram / Twitter / Ask /Google +/ Snapchat / Linkedin – idade mínima para utilização – 13 ANOS
WhatsApp – 13 ANOS
YouTube Kids – 13 ANOS

3.1 Entenda a Criminalização do Bullying no Código Penal

SLM
SIQUEIRA LAZZARESCHI DE MESQUITA
ADVOGADOS

A criminalização do bullying e do cyberbullying ocorreu no Brasil em janeiro de 2024 e precisamos discutir sobre o tema!

Crime de Bullying
146-A. Intimidar sistematicamente, individualmente ou em grupo, mediante violência física ou psicológica, uma ou mais pessoas, de modo intencional e repetitivo, sem motivação evidente, por meio de atos de intimidação, de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais:
Pena - multa, se a conduta não constituir crime mais grave.

Intimidação sistemática virtual (cyberbullying)
Parágrafo único. Se a conduta é realizada por meio da rede de computadores, de rede social, de aplicativos, de jogos on-line ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real:

Pena - reclusão, de 2 (dois) anos a 4 (quatro) anos, e multa, se a conduta não constituir crime mais grave.

O bem jurídico tutelado pelo Artigo 146-A do Código Penal, que trata do crime de intimidação sistemática (bullying), é a **dignidade da pessoa humana**, além da integridade física, psicológica e moral do indivíduo. A lei visa proteger a saúde mental e emocional das pessoas, assegurando o direito de todos a um ambiente seguro, respeitoso e livre de intimidações e abusos.

Especificamente, a norma busca garantir que ninguém seja submetido a situações de humilhação, constrangimento ou discriminação que possam causar dor, angústia e sofrimento. Ao tutelar esses bens jurídicos, a legislação enfatiza a importância do respeito mútuo, da convivência pacífica e da proteção dos direitos individuais em qualquer ambiente, seja ele físico ou virtual.

O sujeito ativo é a pessoa que pratica a conduta descrita como crime na legislação penal, ou seja, o autor do crime. No contexto do Artigo 146-A do Código Penal, que trata do crime de intimidação sistemática (bullying), o sujeito ativo pode ser qualquer pessoa que cometa atos de intimidação, humilhação ou discriminação, de forma repetitiva e intencional, seja em um ambiente físico ou virtual.

No caso específico de bullying escolar, o sujeito ativo pode ser um estudante, professor, funcionário ou qualquer outro indivíduo que, direta ou indiretamente, pratique atos que causem sofrimento à vítima. O conceito é amplo e abrange todos os envolvidos na prática da conduta criminosa, independentemente de sua posição ou status dentro do ambiente onde o bullying ocorre.

O sujeito passivo é a pessoa que sofre a ação criminosa, ou seja, a vítima do crime. No contexto do Artigo 146-A do Código Penal, que trata do crime de intimidação sistemática (bullying), o sujeito passivo é a pessoa que é intimidada, humilhada ou discriminada de forma intencional e repetitiva, sem motivação aparente.
No ambiente escolar ou esportivo, por exemplo, o sujeito passivo pode ser um aluno, um atleta, um professor, ou qualquer outra pessoa que esteja sendo alvo dos atos de violência física, psicológica, moral, social ou virtual. A lei protege o sujeito passivo ao estabelecer penas para os agressores, buscando coibir a prática de bullying e garantir um ambiente seguro e respeitoso para todos.

SEMELHANÇAS ENTRE BULLYING E CONSTRANGIMENTO ILEGAL

- Violação da dignidade: ambos os crimes violam a dignidade da pessoa humana, causando constrangimento, dor ou sofrimento à vítima.
- Uso de violência ou intimidação: os dois delitos envolvem o uso de violência, intimidação ou pressão sobre a vítima, afetando sua liberdade ou integridade.
- Responsabilização penal: tanto o bullying quanto o constrangimento ilegal são crimes punidos pelo Código Penal, refletindo a gravidade dessas condutas na proteção dos direitos individuais.

DIFERENÇAS ENTRE BULLYING E CONSTRANGIMENTO ILEGAL

Repetição das ações: o bullying se caracteriza pela repetição de atos de intimidação ou humilhação ao longo do tempo, enquanto o constrangimento ilegal pode ocorrer em um único ato.

Motivação: no bullying, não há uma motivação evidente; o objetivo é intimidar, humilhar ou discriminar. No constrangimento ilegal, a motivação é forçar a vítima a agir contra sua vontade.

Contexto e forma de abuso: o bullying pode ocorrer tanto em ambientes físicos quanto virtuais (cyberbullying), e envolve um padrão de abuso contínuo. O constrangimento ilegal ocorre em contextos onde há coerção direta e imediata, muitas vezes para obter uma ação específica da vítima.

Penas aplicadas: o bullying, especialmente o virtual, pode ter penas mais severas (reclusão de 2 a 4 anos e multa), enquanto o constrangimento ilegal possui penas menores (detenção de 3 meses a 1 ano ou multa).

O crime de bullying (intimidação sistemática) pode ser absorvido por outros crimes com penas maiores quando as ações cometidas no contexto do bullying configuram delitos mais graves, aplicando-se o princípio da consunção, onde o crime menos grave é absorvido pelo mais grave.

EXEMPLOS DE ABSORÇÃO DO CRIME DE BULLYING POR OUTROS CRIMES MAIS GRAVES:

Lesão corporal ou homicídio: se o bullying envolve agressões físicas que resultam em lesões graves ou na morte da vítima, o crime de bullying é absorvido pelos crimes de lesão corporal ou homicídio, pois a violência física se sobrepõe à intimidação.

Ameaça ou coação: quando o bullying inclui ameaças que visam impedir que a vítima denuncie ou preste depoimento, ele pode ser absorvido pelo crime de coação no curso do processo, com pena maior.

Injúria racial ou racismo: bullying com ofensas raciais configura injúria racial ou racismo, crimes com penas mais severas, que absorvem o bullying.

Crimes sexuais: se o bullying envolve atos que configuram assédio ou importunação sexual, o bullying é absorvido pelo crime sexual, que é considerado mais grave.

Furto: no caso de bullying que envolve o furto de materiais escolares, uniformes ou pertences da vítima, o crime de furto absorve o bullying, especialmente quando a subtração de bens é um meio de intimidar, excluir ou humilhar.

Extorsão: Quando o bullying evolui para ameaças visando obter vantagem econômica, ele pode ser absorvido pelo crime de extorsão.

Instigação ao suicídio: se o bullying ocorre em grupos de WhatsApp/Telegram ou outras redes, levando a vítima a um estado de desespero que culmina em tentativa ou consumação de suicídio, o bullying é absorvido pelo crime de instigação ao suicídio, que possui uma pena muito mais severa devido às consequências graves e irreparáveis para a vítima.

Nesses contextos acima explicados, o bullying é visto como parte do comportamento delitivo mais amplo e grave, sendo absorvido para evitar a duplicidade de punição pela mesma conduta, garantindo que a responsabilização seja proporcional ao dano causado.

3.7 O que é *cyberbullying*, afinal?

De acordo com o parágrafo único da Lei do *Bullying* 13.185/15:

"*Há intimidação sistemática na rede mundial de computadores (**cyberbullying**), quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial*".

Cyberbullying é uma forma de violência contra uma pessoa, praticada pela Internet ou aplicativos de celulares. Praticar *cyberbullying* significa usar o espaço virtual para intimidar e hostilizar uma pessoa (colega de escola, professores, pais de alunos ou mesmo pessoas desconhecidas), difamando, insultando ou ameaçando.

Não há uma quantidade de vezes exatas que a pessoa precisa ser agredida virtualmente para que seja considerado *cyberbullying*. Algumas não ligam quando são humilhadas com apenas um *post* na rede social, mas esse *post* pode ser disseminado de forma incontrolável na rede, causando problemas psicológicos ou, até mesmo, suicídio.

Porque é importante enfatizar o *cyberbullying*?

O *bullying* é caracterizado por ser presencial e restrito a apenas um grupo (colegas de classe, do condomínio, do clube etc.), por isso é possível contê-lo com menos dificuldade. Já o *cyberbullying* acontece via Internet e as agressões podem se espalhar para o mundo inteiro e a remoção do conteúdo por completo é pouco provável, o que poderia afetar não só a vida pessoal, mas também a vida profissional da vítima.

3.7.1 Por que enfrentar o *cyberbullying* tornou-se vital?

Em fevereiro de 2016 entrou em vigor a Lei 13.185/15, que Institui o Programa de Combate à Intimidação Sistemática (Bullying) em todas as instituições de ensino do país, bem como clubes e agremiações recreativas.

A instituição do programa consiste no combate e prevenção constante ao *bullying* (virtual ou presencial). O não cumprimento dessa lei pelos colégios pode ser considerado má prestação de serviço.

A **importância do compliance** no combate ao **bullying** reside na implementação de políticas, normas e práticas que promovem um ambiente ético, respeitoso e seguro, tanto em organizações quanto em instituições, como escolas e empresas. O compliance, que geralmente está relacionado ao cumprimento de leis, regulamentos e padrões éticos, desempenha um papel fundamental na prevenção e no enfrentamento do bullying, inclusive do **cyberbullying**.

SLM

SIQUEIRA LAZZARESCHI DE MESQUITA

ADVOGADOS

Principais Pontos de Importância do Compliance no Combate ao Bullying:

1. **Prevenção e Conscientização**:
   - Programas de compliance promovem a **conscientização sobre o bullying**, educando funcionários, alunos e colaboradores sobre o que constitui bullying e como prevenir e denunciar tais atos. Isso cria uma cultura de respeito e ética.
   - Políticas claras e treinamentos frequentes ajudam a evitar comportamentos inadequados, já que todos são informados sobre as regras e as consequências de violá-las.

2. **Ambiente Seguro e Saudável**:
   - O compliance estabelece normas que garantem a criação de um **ambiente de trabalho ou escolar seguro**, onde todos se sentem respeitados e acolhidos. Quando práticas de bullying são combatidas ativamente, a saúde emocional e o bem-estar dos indivíduos são preservados.
   - Normas de conduta ética são aplicadas para que ninguém tolere comportamentos abusivos.

3. **Detecção e Monitoramento**:
   - Através de mecanismos de compliance, é possível implementar **canais de denúncia** anônimos e seguros, como ouvidorias e sistemas internos, que incentivam as vítimas e testemunhas de bullying a relatar incidentes sem medo de retaliação.
   - Procedimentos de monitoramento e investigação são importantes para detectar sinais de bullying e cyberbullying rapidamente.

4. **Responsabilidade e Sanções**:
   - O compliance define **sanções e medidas disciplinares** claras para aqueles que cometem bullying. Isso desencoraja o comportamento, uma vez que os indivíduos sabem que há consequências formais, como advertências, suspensões ou até desligamentos, dependendo da gravidade.
   - Ele também garante que a organização seja **responsabilizada** caso não atue de maneira adequada diante de denúncias de bullying, o que fortalece o comprometimento em coibir essas práticas.

5. **Proteção Legal e Redução de Riscos**:
   - Para empresas, a implementação de programas de compliance focados em bullying pode reduzir riscos jurídicos, uma vez que a organização estará alinhada com leis trabalhistas e regulamentos que visam proteger

os trabalhadores ou estudantes contra assédio moral e violência psicológica.
- Isso evita potenciais processos por negligência ou omissão em lidar com o bullying, preservando a reputação e os recursos financeiros da instituição.

6. **Cultura Ética e Inclusiva**:
   - O compliance promove uma **cultura organizacional ética**, incentivando a valorização da diversidade e o respeito entre as pessoas, o que naturalmente inibe comportamentos de exclusão e violência, típicos do bullying.
   - Colaboradores e alunos são encorajados a adotar práticas inclusivas, o que reforça o senso de pertencimento e reduz conflitos que poderiam gerar bullying.

A implementação de um programa robusto de compliance no combate ao bullying é crucial para criar um ambiente onde o respeito, a integridade e o comportamento ético são incentivados e mantidos. Além de prevenir e punir o bullying, o compliance proporciona uma estrutura clara para detectar e responder a incidentes, protegendo tanto as vítimas quanto a instituição de possíveis repercussões legais e sociais.

O artigo 20 do Código de Defesa do Consumidor diz que, quando o serviço não é prestado de acordo com a oferta ou apresenta problemas de qualidade, o consumidor pode exigir, alternativamente e à sua escolha, a reexecução dos serviços, sem custo adicional; a restituição imediata da quantia paga, monetariamente atualizada, sem prejuízo de eventuais perdas e danos; ou o abatimento proporcional do preço[1].

Veja nos quadros ao lado os efeitos que causa em vítimas e agressores:

Vítimas

- ☐ Desinteresse e prejuízo na aprendizagem;
- ☐ Evasão escolar ou universitária;
- ☐ Sintomas de ansiedade e/ou depressão;
- ☐ Desenvolvimento de fobia ao ambiente escolar;
- ☐ Pensamentos e prática de suicídio;
- ☐ Ideias obsessivas de vingança;
- ☐ Tentativas e/ou prática de homicídio ou lesão corporal contra o agressor e a comunidade que o cerca.

Agressores

- ☐ Serem alvo ações de reparação civil e/ou ações criminais;
- ☐ Comportamento agressivo crescente com a família e no futuro ambiente de trabalho;
- ☐ Uso abusivo de álcool e outros tóxicos (lícitos e ilícitos);
- ☐ Posse de armas para comprovar seu poder sobre outras pessoas e envolvimento em brigas corporais e "rachas" com veículos.

também que nenhum pai pode impedir a ação da lei.

Além disso, o enfrentamento do problema *cyberbullying* pela Colégio Piaget resultará na diminuição importante da violência social digital nos marcos da Cultura de Paz, assim como cita Lei 13.185/15 e prega o Prof. Daisaku Ikeda:

> *(...) Cabe a nós construirmos um mundo sem guerras. Cada um deve se perguntar se é meramente uma tarefa impossível, ou se deve continuar a desafiar, mesmo em meio às maiores dificuldades – todo o destino do século XXI depende desta decisão." (Daisaku Ikeda, fragmento do ensaio: "Pensamentos sobre a paz")*

PRINCIPAIS RISCOS E ALGUNS EXEMPLOS DE *CYBERBULLYING*: AMEAÇAS/PERSEGUIÇÕES

Os *cyberbullies* utilizam o e-mail ou aplicativos de celulares para enviar mensagens ameaçadoras ou de ódio aos seus alvos. Os agressores podem se fazer passar por outras pessoas, utilizando usernames parecidos com os delas, para envolver outros inocentes no processo de destruição da vítima.

CUTTING - REFLEXO DO *BULLYING* OU MODA NAS REDES SOCIAIS?

Na verdade, ele pode ser muito além disso.

O *cutting* é o termo em inglês para o ato da pessoa se automutilar fazendo pequenos cortes no corpo em lugares que sejam fáceis de esconder. O principal público atingido são jovens do sexo feminino a partir dos 13 anos, as quais usam desse meio para aliviar dores emocionais, como o *bullying*, o *cyberbullying*, problemas com a autoestima, entre outros.

Ademais, essa prática tem se tornado preocupante pela influência causada pelas redes sociais. De acordo com o psiquiatra Olavo de Campos Pinto, membro do International Mood Center e ex-professor da Universidade da Califórnia (EUA), a Internet tem papel preponderante na disseminação atual da prática, que ele chama de epidêmica.

“Nessa idade, a pessoa não tem a personalidade formada e assume um comportamento de grupo altamente perigoso. As redes sociais são multiplicadores, o principal combustível, e (a automutilação) está se tornando uma epidemia. É uma

maneira de lidar de forma impulsiva e destrutiva com frustrações e ansiedades. Tenho visto cada vez mais casos na pré-adolescência. É assustador" — diz Campos Pinto. — Estudos de condução nervosa sugerem que, quando há uma sensação de frustração, o corte alivia a dor psíquica. Há um alívio imediato, mas, quando passa, vem uma sensação de vergonha, de arrependimento, de ser descoberto no seu ato[2].

"Como poceder nos casos de *cutting*?" – Comunique a Direção do Piaget para que sejam tomadas as medidas necessárias, que ajude o aluno e seus pais a enfrentarem essa situação da melhor maneira possível.

3.7.2 Quando alguém pratica *cyberbullying*, que crime de ameaça do código penal ela está cometendo? Esse topico so fazia sentido antes da criminalização, agora tem que ser colocado no comeco do texto, depois dos crimes de pbullying, estalking etx

Art. 147 – Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe **mal injusto e grave**:

Pena – detenção, de um a seis meses, ou multa.
Agressor pode ser qualquer pessoa.
A vítima será a pessoa com capacidade de entendimento da situação.
A ameaça tem que ser verossímil, por obra humana, capaz de instituir receio, independente de causar ou não dano real a vítima.
Trata-se de crime de natureza formal, não sendo necessário que a vítima sinta-se ameaçada e a ameaça estará consumada no instante em que a vítima toma conhecimento do mal prenunciado, independentemente de sentir-se ameaçado ou não.

Calúnia (art. 138 do Código Penal):
Caluniar alguém, imputando-lhe falsamente fato definido como crime:
Pena - detenção, de seis meses a dois anos, e multa.
§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
§ 2º - É punível a calúnia contra os mortos.

Difamação (art. 139 do Código Penal):
Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
Pena - detenção, de três meses a um ano, e multa.

[2] PINTO, Olavo de Campos. Prática de automutilação entre adolescentes se dissemina na internet e preocupa pais e escolas. https://oglobo.globo.com/sociedade/saude/pratica-de-automutilacao-entre-adolescentes-se-dissemina-na-internet-preocupa-pais-escolas-14050535. Acesso 11/07/2017 às 17:39

Injúria (art. 140 do Código Penal):
Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
Pena - detenção, de um a seis meses, ou multa.
§ 1º - O juiz pode deixar de aplicar a pena:
I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
II - no caso de retorsão imediata, que consista em outra injúria.
§ 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

§ 3º Se a injúria consiste na utilização de elementos referentes à raça, cor, etnia, religião, origem ou à condição de pessoa idosa ou portadora de deficiência: (Redação dada pela Lei nº 10.741, de 2003).
Pena - reclusão de um a três anos e multa. (Incluído pela Lei nº 9.459, de 1997).

3.7.3 Roubo de identidade ou de senhas
Ao conseguir acesso ilícito às palavras-passe do seu alvo, o agressor se utiliza dessas para invadir as contas da vítima, causando diversos problemas:

- Por e-mail: Envia mensagens de conteúdo obsceno, pornográfico, agressivo ou violento em nome dela para a sua lista de contatos;
- Por comunicador instantâneo ou em chats: Dissemina boatos, faz-se passar pela vítima e ofende as pessoas com quem fala.

Muitas vezes o agressor entra no perfil de redes sociais onde a vítima tem perfil cadastrado para conhecer os amigos e seguidores; depois altera o perfil de utilizador dessa conta (incluindo, por exemplo, comentários de natureza discriminatória, altera o sexo do usuário no cadastro ou insere itens que possam difamar a imagem do utilizador legítimo da conta), ofendendo terceiros e atraindo a atenção de pessoas mal intencionadas.

O agressor pode depois alterar as senhas e login das contas da vítima, bloqueando o legítimo proprietário ao acesso dessas.

A diferença entre roubo de identidade e fraude de identidade está na forma como cada crime ocorre e no objetivo de quem o comete, embora ambos estejam relacionados ao uso indevido de informações pessoais.

O roubo de identidade ocorre quando alguém obtém e usa ilegalmente as informações pessoais de outra pessoa (como CPF, RG, número de cartão de crédito, senhas, etc.) sem o consentimento dela.

O objetivo principal do roubo de identidade é se apropriar dos dados da vítima. Essas informações podem ser obtidas por diferentes meios, como ataques cibernéticos, phishing, furto de documentos, entre outros.

Exemplo: Alguém acessa o número de seu cartão de crédito e o usa para fazer compras sem sua autorização.

A fraude de identidade, por sua vez, é o ato de usar as informações obtidas, seja de maneira lícita ou ilícita, para cometer uma fraude, ou seja, obter vantagem de forma indevida ou causar prejuízo a alguém.

Enquanto o roubo de identidade se refere ao ato de adquirir os dados, a fraude de identidade está relacionada ao uso desses dados para enganar instituições ou outras pessoas.

Exemplo: Usar o número do CPF de outra pessoa para abrir contas bancárias, pedir empréstimos ou fazer compras no nome dessa pessoa.

Roubo de identidade: Foco na obtenção indevida de informações pessoais. Fraude de identidade: Foco no uso das informações obtidas para cometer atos fraudulentos, causando prejuízo à vítima. Ou seja, o roubo de identidade é o meio e a fraude de identidade é o fim.

Normalmente, esses dois crimes estão interligados, pois quem rouba a identidade geralmente a utiliza para cometer fraudes.

3.7.4 Criação de perfil falso

O adolescente mal-intencionado pode criar uma página pessoal na Internet acerca do alvo dos seus ataques, sem o conhecimento da vítima, na qual insere todo o tipo de informações maldosas ou falsas, além de poder conter dados reais, como a residência, escola, cursos livres e dados pessoais da família da agredido. A seguir, a localização eletrônica é transmitida para uma infinidade de usuários, para que o maior número de pessoas tenham acesso.

Esse tipo de difusão de informação pode ter as características de uma epidemia, espalhando-se rapidamente pelos usuários da rede. Com tantos dados disponíveis, a

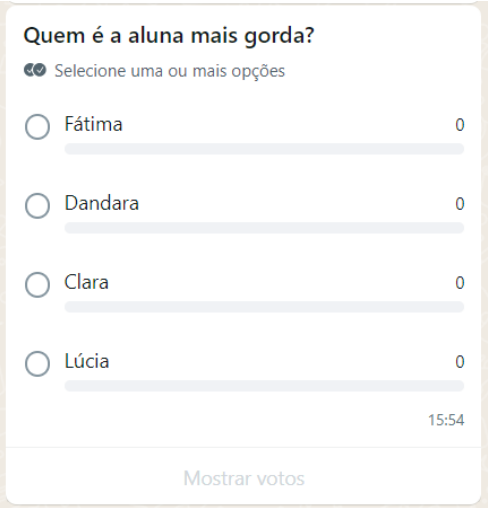
vitima e sua família são alvos fáceis de sequestro, chantagem e ameaças, on-line e off-line.

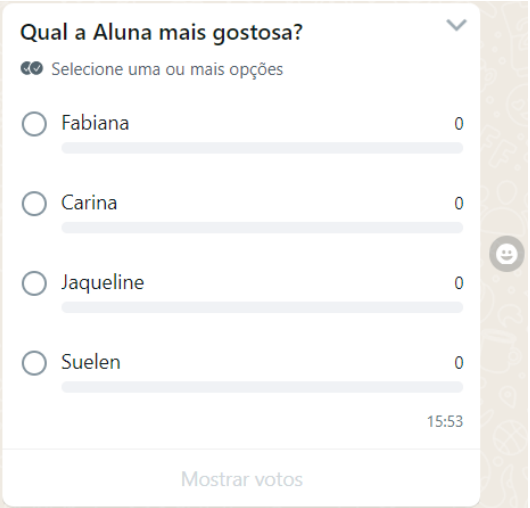
ENVIO DE IMAGENS PELOS MAIS VARIADOS MEIOS

Por vezes o agressor envia mensagens de correio eletrônico em massa, contendo imagens degradantes ou alteradas dos seus alvos. Estas imagens (reais ou adulteradas), podem difundir-se rapidamente, lesando a imagem e o nome da vítima.

SITES/BLOGS DE VOTAÇÃO

Existem vários sites onde é possível votar acerca dos mais variados assuntos, é possível a um jovem criar o tema de "A Mais Feia", "O Mais Gordo", "O Mais Rico", "O Mais Pobre" etc. Exemplo:





ENVIO DE VÍRUS

O envio de vírus não é exclusivo dos adultos. Com a crescente precocidade das crianças e adolescentes, uma forma de prejudicar os seus pares pode ser enviar-lhes vírus para lhes infectar o computador, roubar senhas e/ou login e causar transtornos.
Portanto, quando falamos de segurança móvel, o mais importante é proteger os dados pessoais e a privacidade, bem como evitar que a linha seja indevidamente usada por terceiros.

Na prática, quando se trata de smartphones, os antivírus são colocados em segundo plano e outros recursos, como bloqueio remoto e exclusão de dados, ganham mais relevância, já que é muito mais fácil perder um smartphone, e assim deixar seus contatos, mensagens e chamadas expostos.

Celulares infectados costumam apresentar alguns sintomas que podem ajudá-lo a evitar de ter sua privacidade violada. Entre as ocorrências mais comuns, estão:

- A repentina diminuição da vida útil da bateria;
- Utilização indevidamente do recurso de Bluetooth para enviar arquivos infectados para outros aparelhos;
- Reinicialização do celular sem solicitação;
- Surgimento de arquivos corrompidos;
- Desconfiguração de botões de comandos;
- Dificuldade para desligar o celular;
- Consumo de créditos, aumento excessivo da conta e/ou consumo de dados (isso acontece por trojans enviarem mensagens para sua lista de contatos, sem que você tenha pedido por isso); e,
- De maneira menos perceptível, coletar informações sigilosas[3].

O melhor é ter sempre um bom antivírus instalado, mas se isto ainda não for o suficiente, outras medidas adicionais podem ajudar a evitar infecções no seu aparelho celular:

- Não faça o desbloqueio do dispositivo, técnica conhecida como "root";
- Configure uma senha para desbloquear a tela do aparelho;
- Prefira sempre aplicativos de confiança, de preferência os da loja oficial;
- Não use redes Wi-Fi públicas para qualquer tipo de transação bancária;
- Revise periodicamente as permissões que os apps solicitam; e,
- Armazene no dispositivo apenas dados confidenciais que sejam indispensáveis.

São pequenas medidas que garantem a vida útil de seu equipamento e acima de tudo e mais importante, a privacidade do indivíduo quanto às informações existentes nestes equipamentos[4].

---

[3] Disponível em http://www.tecmundo.com.br/seguranca/23080-como-saber-se-meu-celular-esta-infectado.htm Acesso em: 06 Fevereiro de 2015

[4] Disponivel em < http://info.abril.com.br/noticias/blogs/download-da-hora/seguranca/5-antivirus-para-celular-e-porque-voce-precisa-deles/ Acesso em: 06 Fevereiro de 2015
Disponivel em < http://www.techtudo.com.br/kits/aplicativos-antivirus-para-android.html> Acesso em: 06 de Fevereiro de 2015

INSCRIÇÕES EM NOME DA VÍTIMA DE VÍRUS

É perfeitamente possível um usuário da Internet inscrever-se num determinado site usando os dados de outra pessoa. Os locais escolhidos costumam ser sites de pornografia, fóruns de conteúdo discriminatório ou outros que sejam contrários à ideologia da vítima. O resultado desta prática é o excesso e-mail que não são do seu interesse (SPAM), podendo os mesmos até ser nocivos (veja *phishing scam*).

CONSTRANGIMENTO ILEGAL

O crime de constrangimento ilegal, previsto no artigo 146 do Código Penal Brasileiro, consiste em obrigar alguém, mediante violência ou grave ameaça, a fazer ou não fazer algo, ou a tolerar que se faça algo contra a sua vontade. A pena prevista é de detenção de três meses a um ano, ou multa, podendo ser aumentada caso haja uso de violência.

Art. 146 - Constranger alguém, mediante violência ou grave ameaça, ou depois de lhe haver reduzido, por qualquer outro meio, a capacidade de resistência, a não fazer o que a lei permite, ou a fazer o que ela não manda:

Pena - detenção, de três meses a um ano, ou multa.

Aumento de pena

§ 1º - As penas aplicam-se cumulativamente e em dobro, quando, para a execução do crime, se reúnem mais de três pessoas, ou há emprego de armas.

§ 2º - Além das penas cominadas, aplicam-se as correspondentes à violência.

§ 3º - Não se compreendem na disposição deste artigo:

I - a intervenção médica ou cirúrgica, sem o consentimento do paciente ou de seu representante legal, se justificada por iminente perigo de vida;

II - a coação exercida para impedir suicídio.

Divulgação de segredo

Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:

Pena – detenção, de um a seis meses, ou multa.

§ 1º Somente se procede mediante representação.

§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: (Incluído pela Lei nº 9.983, de 2000)

Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa

§ 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

3.8 USO EXAGERADO DA INTERNET

Para saber reconhecer o limite do uso da Internet, é preciso estar atento a 4 características importantes:

- Uso de dispositivos digitais por muito tempo seguido, deixando de dormir ou de fazer as tarefas escolares para ficar conectado até tarde da noite;
- O usuário não consegue controlar o uso, apenas pensa em continuar conectado e quando não está, só pensa na hora em que poderá usar o computador/tablet /celular;
- Esse uso se torna repetitivo, apesar de parecer prazeroso. A criança/adolescente é capaz de ficar horas a fio no mesmo jogo, dias seguidos fazendo a mesma coisa. O uso do computador/ tablet /celular fica pouco criativo;
- Deixa tudo de lado para estar conectado ou jogando, deixando de encontrar os amigos presencialmente e postergando as atividades curriculares e extracurriculares. O uso descontrolado de games é uma das formas de fuga de problemas para se sentir melhor, esquecendo algo que não está bem ou que não sabemos como lidar. Porém, essa não é a alternativa para lidar com as dificuldades.

Conversar sobre a importância da prática de exercícios, atividades físicas e encontros com os amigos da escola, pessoas do convívio diário da criança/adolescente. A

interação na vida real é muito mais interessante do que uma simples conversa ou discussão na web.

A atividade extracurricular chamada como DETOX DIGITAL proporciona ao aluno a desconexão do mundo virtual e abandonando, temporariamente, qualquer tipo de tecnologia: celular, carregador e até relógio. É um excelente caminho para manter o equilíbrio entre saúde, produtividade e eficiência do aluno em um mundo conectado. Ao fazer uma desintoxicação digital tem-se a chance para uma pausa e recarregar as energias e sintonizando com a natureza, amigos e familiares.

3.9 Sofri *cyberbullying* dos meus alunos, o que faço?

- Não revide com insultos e nem comece uma briga virtual com discentes ou pais;
- Faça o Print Screen da tela. Salve a imagem e imediatamente encaminhe para a diretoria/coordenação para avaliação do caso com os profissionais da área jurídica;
- Converse com a coordenação quais serão as medidas que a Colégio Piaget prevê tomar em relação, de acordo o Guia do Professor.

3.9.1 Como devo proceder se meu aluno veio desabafar comigo sobre o *cyberbullying* que está sofrendo?

- Ampare o aluno e deixe-o desabafar;
- Em seguida, leve-o para a coordenação para tomar as devidas providências que estão no estatuto do colégio;
- Chame para conversar os pais dos adolescentes envolvidos, na presença do coordenador ou diretor.

Sabemos hoje em dia que o compliance escolar, é uma ferramenta de proteção dentro das instituições de ensino, podemos dizer que de todos os atores que dentro do estabelecimento se encontram em atividade escolar, podem se precaver de eventuais problemas, como danos materiais e morais.

Existem várias leis que estão ligadas ao assunto, muitas já foram citadas aqui, A lei como a PNED, Lei 14.533/2023, Política Nacional de Educação Digital, essa lei alterou alguns dispositivos da LDB Lei 9.394/96, lei base da educação nacional, e a LGPD, mais voltado para educação e desenvolvimento de práticas de uso de TIC (tecnologia de informação e comunicação), que tem um caráter de Política Nacional e a Lei de combate ao Bullying, com uma característica punitiva.

3.2 A Importância do direito autoral

O direito autoral assume importância significativa nos dias atuais, como já se mostrou no século XX, considerado como o "século da propriedade intelectual"[5]. Na atualidade, tal relevância torna-se mais acentuada em decorrência dos fantásticos aparatos tecnológicos na área de comunicação, especialmente, na chamada "Sociedade da Informação"[6]. Na visão jurídica, essa temática[2] dá ênfase à liberdade de expressão, que é amparada firmemente por um de seus maiores protetores: o Estado Democrático Brasileiro.

O direito do autor também possui grande importância, dada a sua abrangência: da produção literária, de importância inquestionável ao mais incauto, às artes em geral, tão necessárias para a humanidade. Fotografia, escultura, litografia, cartografia, músicas com ou sem letra, projetos de engenharia e arquitetura são apenas alguns exemplos. Dessa perspectiva, resulta ser uma área que desperta tanto interesse[7].

3.3 Cuidado ao Indicar Sites para Estudos

Indicar sites para que os alunos façam pesquisa é normal nos dias de hoje. Mas você lê o termo de uso do site?

Apesar de parecer inofensivos, alguns sites limitam a idade de seus visitantes por conter imagens e cenas que não são considerados apropriados para menores de 13 ou 16 ou 18 anos.

Outro ponto a se atentar são termos sugeridos para os alunos pesquisarem na Internet. Antes de indicar algum conteúdo para ser pesquisa na web, faça a busca primeiro para conferir se não virá algum resultado inapropriado para a faixa etária dos alunos. Ficou com dúvida se o conteúdo pode ser apropriado ou não? Consulte a Coordenação Pedagógica ou a Direção.

---

[5] ADOLFO, Luiz Gonzaga Silva. Algumas reflexões sobre a importância da propriedade intelectual no século XX. Revista Estudos Jurídicos, São Leopoldo, n. 78, p. 113-25, jan./abr. 1997.

[6] ASCENSÃO, José de Oliveira. A Sociedade da informação. Direito da sociedade da informação, Coimbra, vol.1, p.163-184: "Sociedade da Informação não é um conceito técnico: é um slogan. Melhor se falaria até em sociedade da comunicação, uma vez que o que se pretende impulsionar é a comunicação, e só num sentido muito lato se pode qualificar toda a mensagem como informação. Entre as mensagens que se comunicam há as que são atingidas por um direito de autor ou direito conexo, criando-se um exclusivo."

[7] Nesse sentido, o entendimento de D. Manoel Gonçalves Cerejeira, citado por Antonio Chaves (Direito de autor: princípios fundamentais. São Paulo: Forense, 1987, p. 4): "Considero o direito de autor um dos direitos sagrados, se posso exprimir-me assim. Cumpre zelá-lo e defendê-lo. Nada mais belo que a criação intelectual. Se fosse possível, devia ser pago em mirra, incenso ou ouro".

3.5 Sobre os Comunicadores Instantâneos (Telegram/WhatsApp)

Esses comunicadores são aplicativos para computadores, celulares ou tablets que viabilizam a comunicação entre seus usuários em tempo real, permitindo o envio e recebimento de mensagens, fotos, vídeos e arquivos digitais.

Esses aplicativos são ótimos para manter as pessoas conectadas. No entanto, eles trazem grandes riscos. Veja a seguir quais são os perigos e como preveni-los:

A) PREJUÍZO DE IMAGEM E DANO MORAL

WhatsApp é um aplicativo muito usado no Brasil, mas atenção com as visualizações únicas de imagens trocadas, pois existem aplicativos que mesmo apagado o conteúdo ele pode reexibir.

Cuidado com as imagens (foto, vídeo e arquivos) que disponibiliza nos aplicativos, pessoas de má-fé podem capturar e divulgar essas imagens sem autorização, causando sofrimento ao usuário do aplicativo.

Atenção com os grupos de conversas. Pondere antes de escrever ou enviar algo neste grupo, pois sempre há a chance do “engraçadinho” encaminhar mensagens suas para outras pessoas.

Certifique-se de que está falando com a pessoa certa - Além de criminosos virtuais, é preciso ter cuidado com aqueles que também agem nas ruas, roubando celulares. Há casos de pessoas que têm o celular subtraído e o criminoso troca mensagens com os contatos da vítima fingindo ser ela, para aplicar um golpe. Portanto, não passe dados pessoais e não marque encontros sem antes confirmar por ligação.

Sempre bloqueie seu smartphone, computador ou tablet com senha de acesso (numérica, por reconhecimento de padrão ou biométrica).

Atenção - Não existe “segredo” em comunicadores instantaneos. Se deseja uma conversa sigilosa, fale pessoalmente.

O Colegio Piget SBC recomenda que os seus colaboradores nunca forneçam dados pessoais para alunos e responsaveis legais. É importante que todos da comunidade escolar apenas usem os canais oficiais de comunicação, sendo certo que o WhatsApp e Telegram não são canais reconhecidos pelo Colegio Piaget SBC.

B) VÍRUS

Antes de fazer download de arquivos, verifique se o remetente é conhecido. Não responda para números desconhecidos, essa é uma forma de golpe na qual o criminoso manda uma mensagem, e qualquer retorno serve para a apropriação de dados. Por isso, instale antivírus.

Evite também Wi-Fi público, onde a senha é compartilhada e pessoas mal intencionadas podem espionar o tráfego.

C) *SEXTING*

Sexting (contração de *sex* e *texting*) é o ato de enviar mensagens ou fotos sexualmente explícitos de forma eletrônica, principalmente entre smartphones. Não peça imagens sensuais e, se lhe for solicitado, não as forneça. Recuse passar adiante mensagens de *sexting* e diga claramente para os amigos pararem com o *sexting*. Bloqueie a comunicação com amigos que enviam mensagens de *sexting*.

Se você conhece algum aluno que está enviando fotos sexualmente reveladoras ou alguém que as tenha, informar o ocorrido para o site de hospedagem/rede social e a Direção do Colégio Piaget. Fenômeno do *sexting* é de preocupação pública devido os riscos de estimulo a pornografia infantil e a pedofilia.

D) PEDOFILIA

Pedófilos são pessoas adultas (homens e mulheres) que têm preferência sexual por crianças – meninas ou meninos - do mesmo sexo ou de sexo diferente, geralmente que ainda não atingiram a puberdade ou no início da puberdade.

Artigo 241-B do ECA - é considerado crime o ato de "adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente."

Nas salas de bate-papo, aplicativos de comunicação instantânea ou redes sociais eles adotam um perfil falso e usam a linguagem que mais atrai a faixa etária que deseja contato. Infelizmente não é fácil reconhecer um pedófilo, porque geralmente é uma pessoa aparentemente comum e não possui características físicas que as diferenciem das demais. Alguns comportamentos são comuns entre esses criminosos, como[8]:

[8] http://www.turminha.mpf.mp.br/direitos-das-criancas/ 18-de-maio/como-identificar-o-pedofilo

- Gostam de ficar sozinhos com crianças ou adolescentes, sendo muito atenciosos e sedutores;
- Gostam de fazer "amizade" com criança/adolescente;
- Sempre procuram agradar sua vítima com presentes, elogios e promessas;
- Em suas casas possuem vários objetos, jogos, guloseimas para agradar crianças e adolescentes;
- Procuram fazer carinho nas partes íntimas de crianças e adolescentes;
- Sempre pedem para guardar segredo e nunca contar nada a ninguém sobre seus comportamentos;
- Às vezes, ameaçam a criança/adolescente, algo ou alguém de que goste muito, caso não ceda às suas vontades;
- Pedem para filmar ou tirar fotos de criança/adolescente, com pouca ou nenhuma roupa e pedem para fazer poses sensuais.

A partir da Lei 12.015/09, que modificou o Código Penal em relação aos crimes sexuais, o estupro (sexo vaginal mediante violência ou ameaça) e o atentado violento ao pudor (outras práticas sexuais) foram fundidos no crime de estupro e todo ato sexual com pessoas com menos de 14 anos passou a configurar estupro de vulnerável, ainda que o menor concorde com o ato. Veja a lei:

E) Estupro de Vulnerável

> Art. 217-A. Ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 (catorze) anos:
> Pena - reclusão, de 8 (oito) a 15 (quinze) anos.
> § 1º Incorre na mesma pena quem pratica as ações descritas no caput com alguém que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, ou que, por qualquer outra causa, não pode oferecer resistência.
> § 2º (VETADO)
> § 3º Se da conduta resulta lesão corporal de natureza grave:
> Pena - reclusão, de 10 (dez) a 20 (vinte) anos.
> § 4º Se da conduta resulta morte:
> Pena - reclusão, de 12 (doze) a 30 (trinta) anos.

É importante que os pais naveguem na Internet com os filhos, para que saibam os sites preferidos, os programas que ele usa e as atividades que faz enquanto está on-line. Explicar para crianças e adolescentes que não devem conversar com estranhos na Internet ou nos aplicativos. **NUNCA** eles devem fornecer informações pessoais como nome, endereço e escola em que estuda em conversas. **NUNCA** enviar fotos para

pessoas que conheceram pela Internet e a não receber dessas pessoas nenhum tipo de arquivo. **NUNCA MARCAR ENCONTROS COM DESCONHECIDOS**.

É importante que os pais conheçam os amigos do mundo virtual e evitem em colocar o computador no quarto da criança/adolescente.

3.6 Cuidado com *Phishing Scam*

É uma modalidade de fraude digital, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, login, dados financeiros como número de cartões de crédito e outros dados pessoais. Como o nome propõe, é uma tentativa de um fraudador tentar "pescar" - do inglês *fishing* - informações pessoais de usuários.

As redes sociais são muito utilizadas para esse fim, por se tratar de meio onde circulam fotografias, informações da vida alheia, e onde estabelecem-se paralelos com o mundo real. Os ataques acontecem:

- Via e-mail;
- Via website;
- Via mensagens instantâneas;
- Via *malware*.

Prevenção - Alguns cuidados ao ler e-mails e mensagens de qualquer natureza: Verifique o remetente do e-mail e nunca baixe e nem execute arquivos não solicitados.

Segurança na Internet (website) - antivírus atualizado no seu computador; verifique se o seu sistema operacional (ex. Windows/IOS) está atualizado; e certifique-se se o firewall está instalado e habilitado.

3.9.2 – Qual a importância da LGPD para o Colégio Piaget?

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, é uma legislação brasileira que regula o tratamento de dados pessoais de cidadãos, tanto no meio físico quanto no digital. O objetivo principal é garantir a privacidade e a segurança dos dados, dando aos titulares maior controle sobre como suas informações são usadas e armazenadas.

SLM

SIQUEIRA LAZZARESCHI DE MESQUITA

ADVOGADOS

Por que a LGPD é importante para o Colégio Piaget?

O Colégio Piaget lida com um grande volume de dados pessoais e sensíveis, tais como:

- Informações de alunos (nome, endereço, notas, histórico escolar);
- Dados dos pais ou responsáveis (contatos, situação financeira);
- Dados de saúde (atestado médico; medicações)
- Dados de professores e funcionários (CPF, RG, endereço, salários).

A LGPD exige que esses dados sejam tratados de forma responsável e segura. O Colégio Piaget, como responsável pelo tratamento desses dados, adota medidas para garantir a privacidade de todos por meio da implementação do projeto de proteção de dados.

A LGPD é uma lei fundamental para garantir a privacidade e a proteção dos dados de todos os cidadãos. Para o Colégio Piaget, ela representa uma responsabilidade de tratar as informações de alunos, pais e funcionários de maneira segura, transparente e ética.

Adotar boas práticas de proteção de dados não só evita sanções, como também fortalece a relação de confiança entre a instituição e a comunidade escolar.

Em razão desse cuidado com o toda comunidade escolar é que o Colégio Piaget Implementou os passos para adequar sua escola à LGPD, tais como:

Mapeamento de Dados
A escola deve identificar todos os dados pessoais que coleta, o motivo da coleta e como esses dados são tratados.

Revisão de Políticas e Procedimentos
Revisar contratos, formulários de matrícula e políticas internas para garantir que estão em conformidade com a LGPD.

Treinamento de Funcionários
É essencial que todos os colaboradores, professores e funcionários sejam treinados sobre a importância da proteção de dados e as práticas que devem ser adotadas para garantir a conformidade com a lei.

Implementação de Medidas de Segurança
Instalar sistemas de segurança digital, como criptografia de dados e controle de acesso. Para documentos físicos, garantir o armazenamento seguro em arquivos trancados.

Encarregado de dados

SLM

SIQUEIRA LAZZARESCHI DE MESQUITA

ADVOGADOS

Designou o escritório de advocacia Siqueira Lazzareschi de Mesquita Advogados para atuar como Encarregado de Proteção de Dados para monitorar a conformidade com a LGPD e ser o ponto de contato com a ANPD.

Qualquer duvida e/ou solicitação sobre a proteção de dados do Colegio Piaget SBC, favor entrar em contato no email contato@slmadv.com.br

DEVER DE SIGILO DO COLABORADOR DO COLEGIO PIAGET

Toda informação relativa à saúde do aluno e ao seu rendimento escolar é considerada dado sensível pela Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018). Esses dados incluem condições médicas, notas, comportamento e qualquer outra informação pessoal que, se divulgada sem autorização, pode expor o aluno a constrangimentos e discriminação. A LGPD exige que o tratamento desses dados seja feito com consentimento explícito e para finalidades legítimas, como a gestão escolar e o bem-estar do aluno.

Consequências da divulgação indevida de dados de alunos ou familiares de alunos

Sanções trabalhistas: a divulgação não autorizada dessas informações pelo colaborador pode resultar em advertência, suspensão ou demissão por justa causa, devido à violação do dever de sigilo profissional e à quebra de confiança, prerequisito básico para a atuação em um ambiente repleto de menores de idade.

Responsabilidade civil: os responsáveis legais do aluno podem ingressar com ações civis contra o colaborador, requerendo indenizações por danos morais e materiais causados pela exposição indevida de informações sensíveis. Isso se deve ao impacto negativo na vida do aluno, incluindo constrangimento e prejuízos emocionais.

Responsabilidade penal: a divulgação de dados sensíveis, como questões de saúde ou rendimento escolar, pode configurar crimes como violação de segredo (Art. 153 do Código Penal) e, em casos graves, instigação ao cyberbullying. A exposição de informações em redes sociais, grupos de WhatsApp ou outros meios digitais pode incitar comentários ofensivos, perseguições virtuais e ataques que afetem ainda mais o menor.

Cyberbullying: a divulgação de dados pessoais e sensíveis pode resultar em cyberbullying, aumentando o sofrimento da vítima. O autor pode responder por esse crime, com pena de reclusão de 2 a 4 anos e multa, quando realizado por meio digital, conforme previsto no Artigo 146-A do Código Penal.

Essas implicações demonstram que a divulgação de informações sensíveis dos alunos sem autorização não só viola a LGPD como expõe educadores a graves consequências legais, civis e criminais, reforçando a importância do uso responsável e ético dos dados para proteger os direitos e a dignidade dos menores.

4.0 – O QUE É COMPLIANCE ESCOLAR?

O compliance escolar refere-se ao conjunto de práticas e políticas implementadas por uma escola para garantir que ela cumpra as normas legais e regulatórias, assim como os padrões éticos e morais. Isso envolve o respeito a leis de educação, diretrizes de segurança, políticas internas, e princípios de integridade.

Objetivos do Compliance Escolar:

Assegurar conformidade legal: O compliance escolar assegura que a escola siga todas as leis e normas aplicáveis, como as diretrizes educacionais, trabalhistas, de segurança e de proteção de dados. Isso evita penalidades legais e assegura o funcionamento correto da instituição.

Promover a ética: Ele estabelece um código de conduta e orienta comportamentos éticos entre alunos, professores, administradores e todos os envolvidos. Isso ajuda a criar um ambiente de respeito, integridade e transparência.

Garantir a transparência: O compliance promove a transparência nas decisões e nos processos da escola, tornando as informações acessíveis e garantindo que pais, alunos e funcionários estejam cientes dos procedimentos e políticas adotadas.

Proteger os alunos e funcionários: O compliance escolar protege os direitos de todos os membros da comunidade escolar, garantindo que não haja discriminação, assédio ou qualquer outro tipo de violação. Ele também zela pela segurança e bem-estar físico e emocional dos alunos e funcionários.

Quando a escola opera de forma ética e em conformidade com as normas, cria um ambiente de confiança e respeito, o que contribui diretamente para uma melhor qualidade no processo de ensino-aprendizagem.

COMO FUNCIONA O CANAL DE DENUNCIA DO PIAGET?

Um canal de denúncia digital é uma plataforma online desenvolvida para instituições de ensino, facilitando a comunicação segura entre a escola e a comunidade escolar,

incluindo alunos e pais. Essa ferramenta é essencial para gerenciar e resolver as questões que surgem nos grupos de WhatsApp de mães e alunos, um dos principais pontos de tensão e conflito dentro do ambiente escolar.

O canal de denúncia permite que reclamações, sugestões, denúncias e elogios sejam enviados de forma organizada, seja anonimamente ou não, garantindo privacidade e a segurança no tratamento dessas informações. O Colégio Piaget oferece um meio eficiente e acessível para que todos dentro do ambiente educacional possam expressar suas preocupações e contribuir para um clima de maior compreensão e respeito mútuo.

Adotar nosso canal de ouvidoria digital significa proporcionar uma ferramenta valiosa para resolver rapidamente problemas de comunicação, melhorando assim a qualidade do ambiente educacional e promovendo uma cultura de paz e respeito entre todos os envolvidos.

O Processo de Gestão de Solicitações é desenhado para maximizar a eficiência e a clareza na maneira como as escolas lidam com reclamações e denúncias. Este processo inclui várias ferramentas que facilitam uma resposta rápida e informada a qualquer questão que possa surgir dentro do ambiente escolar. Aqui está como isso funciona:

1.Gráficos Ilustrativos e Simples: A plataforma exibe dados visuais fáceis de entender, que resumem as reclamações recebidas. Esses gráficos permitem que os administradores vejam rapidamente as tendências de problemas, frequência de queixas específicas, e outras métricas relevantes. Esta visão geral visual ajuda a escola a identificar áreas problemáticas que podem necessitar de atenção adicional, permitindo intervenções focadas e bem-informadas.

2.Estatísticas Precisas: Fornece estatísticas detalhadas sobre todos os aspectos das reclamações processadas. Isso inclui informações sobre o tempo de resposta, tipos de reclamações, e eficácia das resoluções adotadas. Tais dados são cruciais para avaliar o desempenho da escola no manejo de questões internas e ajustar procedimentos conforme necessário para melhorar a eficácia das respostas.

3.Sistemas de Alerta para Rápida Intervenção: A plataforma está equipada com sistemas de alerta que notificam imediatamente os administradores sobre denúncias graves ou questões urgentes. Isso assegura que a equipe escolar possa agir prontamente para resolver tais problemas, minimizando possíveis danos ou escaladas de conflitos. Esses alertas são fundamentais para manter um ambiente escolar seguro e acolhedor, pois garantem que nenhuma questão crítica passe despercebida.

Para que toda essa gestão funcione de forma eficiente é necessário um **Canal de denúncias:** Implementar um canal seguro e confidencial para que qualquer pessoa possa reportar violações de normas e condutas antiéticas.

5.0 – Política Nacional de Cibersegurança (PNCiber) – DECRETO nº 11.856, DE 26 DE DEZEMBRO DE 2023

A Política Nacional de Cibersegurança (PNCiber), instituída no Brasil, tem como objetivo fortalecer a segurança cibernética do país e proteger as infraestruturas críticas contra ameaças digitais. Ela define diretrizes estratégicas para promover a segurança de informações no ambiente digital e mitigar riscos que possam comprometer sistemas escolares, empresariais e pessoais.

A implementação da Política dentro da Instituições de ensino se faz necessária em razão das diversas plataformas digitais que elas operam de ensino online, sistemas de gestão acadêmica e redes internas. É responsabilidade das instituições:

- Garantir a segurança das plataformas utilizadas para aulas virtuais, e-mails e aplicativos de comunicação, protegendo contra invasões, vazamento de dados e cyberbullying;
- Verificar a segurança de softwares e aplicativos utilizados;
- Proteger a rede de comunicação da escola, com o uso de firewalls e outros mecanismos de segurança digital;

O colégio Piaget têm um papel fundamental em educar alunos e funcionários sobre boas práticas de cibersegurança. Isso inclui:

- Promover treinamentos e workshops para conscientizar sobre riscos digitais, como phishing, ataques de malware e invasões de privacidade;

- Ensinar alunos a navegar com segurança na internet, proteger suas senhas e dados pessoais, e a identificar comportamentos online arriscados.

Canais de denúncias de crimes digitais

Associação de Serviço de Orientação e Suporte às Vítimas do Bullying – SOS Bullying
Site: https://sosbullying.org/
E-mail: contato@sosbullying.org

SLM

SIQUEIRA LAZZARESCHI DE MESQUITA

ADVOGADOS

Endereço: Avenida Paulista, nº 1471, conjunto 511, sala 4730, Bela Vista, Cep: 01.311-927
Instagram: @sosbullyingbr
Delegacia de cybercrimes no Brasil https://new.safernet.org.br/content/delegacias-cibercrimes
Denúncia da policia federal: https://www.gov.br/pf/pt-br/canais_atendimento/comunicacao-de-crimes
Denúncia no Google: https://support.google.com/
Grupo Meta: https://compliance.meta.com.br/denuncia/
TikTok: https://support.tiktok.com/en/safety-hc/report-a-problem

Realização
Siqueira Lazzareschi de Mesquita Advogados

Apoio
ASSOCIAÇÃO DE SERVIÇO DE ORIENTAÇÃO E SUPORTE ÀS VÍTIMAS DO BULLYING