



GUIA PARTICIPATIVO DE SEGURANÇA DA INFORMAÇÃO NAS ESCOLAS ESTADUAIS

VERSÃO 1.0
Novembro de 2015

SECRETARIA DE
EDUCAÇÃO



Expediente

GOVERNO DO ESTADO DE MINAS GERAIS

Governador do Estado de Minas Gerais
Fernando Damata Pimentel

Vice-governador do Estado de Minas Gerais

Antônio Eustáquio Andrade Ferreira

Secretaria de Estado de Educação
Macaé Maria Evaristo dos Santos

Secretário Adjunto de Estado de Educação

Antônio Carlos Ramos Pereira

Subsecretaria de Informações e Tecnologias Educacionais
Júnia Sales Pereira

Subsecretaria de Educação Básica
Augusta Aparecida Neves de Mendonça

Equipe responsável pela versão 1.0
Superintendência de Tecnologias Educacionais

André Luiz Rodrigues
Ângelo Viegas de Carvalho Ruas
Corina Soares Giovanini
Edmara Magalhães Pereira
Estael Lúcia Vasconcelos
Josiane França e Braga
Suely da Piedade Alves

Diagramação

Edmara Magalhães Pereira

Desenhos e Arte

Ângelo Viegas de Carvalho Ruas

FALE CONOSCO – 0800 970 1212

Você no Guia Participativo de Segurança da Informação da SEE



Esse Guia Participativo de Segurança da Informação nas Escolas será ilustrado e complementado por meio da participação de alunos enviando-nos charges, desenhos ou imagens até 30 de junho de 2016, bem como sugestões do seu conteúdo.

É importante que as charges, desenhos, imagens e sugestões sejam de sua própria autoria e sobre temas de Segurança da Informação.

A SEE-MG realizará Rodas de Conversas de validação e melhoria do Guia em 2016. Se a sua escola quer participar, formalize o seu interesse até o dia 04 de Abril de 2016.

Informações sobre esse processo no site:

<http://portal.educacao.mg.gov.br/>

Temas

A Internet como Espaço Público

Navegar é Preciso, mas com Segurança

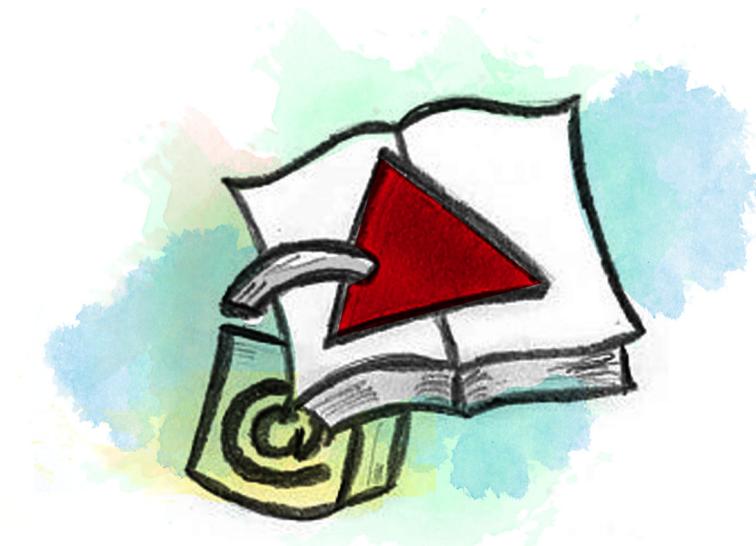
Redes Sociais e Uso Consciente

Ciberbullying e Sexting

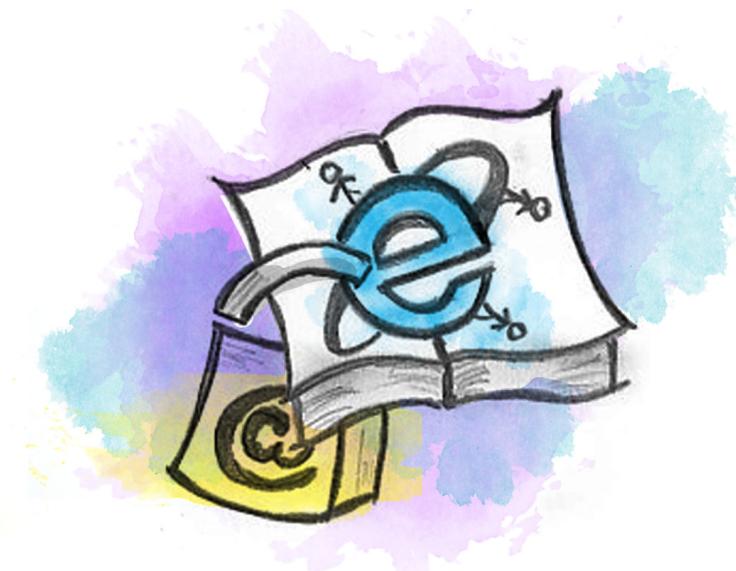
Privacidade e Aliciamento

Canais de Denúncia

Uso do Celular nas escolas: Vilão ou Aliado?



A internet como espaço público



Internet é um grande espaço público em que milhares de pessoas entram e saem a todo momento, compartilhando informações das mais variadas formas, sejam elas imagens, textos e vídeos, em todas as partes do planeta. Para que tudo isso seja possível, a principal forma de propagação desse conteúdo é um sistema globalizado de computadores, em que todas as informações são armazenadas e disponibilizadas.

Porém, esta grande rede mundial de informações não é simplesmente uma praça ou rua por onde você pode transitar

livremente. A internet pode ser uma ferramenta útil para fazer pesquisas, estudar, jogar e compartilhar informações, mas esse ambiente virtual também pode deixar os usuários expostos a uma série de riscos. Assim, ela institui direitos e deveres para quem a utiliza, como forma de entretenimento ou mesmo profissionalmente, com o objetivo de oferecer segurança às informações.

O uso da internet com segurança também dentro da sala de aula está cada vez mais presente no cotidiano dos alunos, uma vez que ela se tornou um dos principais espaços de comunicação entre os adolescentes. Tudo o que acontece no mundo é disponibilizado na internet e, muitas vezes, há dúvida do que comentar, ou quais sites acessar, assim como quais comportamentos assumir para prevenir-se de riscos que ela oferece.

Seguindo uma lista dos vários direitos do usuário na internet, pode-se citar principalmente o direito de acesso à informação e à tecnologia, bem como o direito de expressar-se livremente e dar opinião nos assuntos que interessam. Tendo o direito de ser protegido e não ser discriminado. Além disso, o direito à educação e ao acesso às oportunidades que as novas tecnologias oferecem para a formação pessoal e profissional. O direito à intimidade - quando dados pessoais e imagem são divulgados na internet, sem permissão. E, para finalizar, há o direito de se divertir e de jogar na internet ou em outras novas tecnologias.

Mas todo direito vem acompanhado de um dever, alguns cuidados são importantes para se prevenir do mau uso da internet, como: não baixar música de lugares não autorizados e não acessar sites desconhecidos com conteúdos impróprios. Tenha cuidado ao usar as redes sociais: não poste mensagens com duplos sentidos, ofensivas e racistas, não publique imagens de cunho sexual ou erótico e jamais escreva algo que não seja verdadeiro sobre qualquer pessoa. Jamais plagiar ou copiar algo publicado na web de outras pessoas também faz parte dos cuidados a serem tomados.

Os avanços que a internet vem trazendo cada vez mais para o mundo e a velocidade das informações provocam inúmeras transformações e permitem desvendar esse espaço público virtual, mas também existem riscos que são danosos à sociedade e que podem ser evitados, quando utilizadas as regras de segurança. Saber fazer um bom uso da internet pode ajudar a trilhar os vastos caminhos públicos, nunca antes conhecidos , criando espaço de forma segura.

Navegar é preciso, mas com segurança



A necessidade de utilização da internet hoje é inevitável. Fazemos buscas incessantes dos mais variados assuntos na rede, onde é importante nos preocupar onde “estamos pisando”. O acesso pode ocorrer em casa, na escola, no trabalho e em ambientes externos como uma lan house, onde os equipamentos são usados por muitas pessoas.

Muitas vezes necessitamos de algum software ou aplicativo para resolver algumas questões de trabalho, estudos ou até mesmo de entretenimento. Para isso, há a necessidade de instalação do mesmo. É comum que nos permitam utilizá-los e, sem perceber,

juntamente com a instalação vem algo que pode nos prejudicar, como “malware” (que captura informações do usuário). Escolha sempre aplicativos e softwares com cuidado e dê preferência àqueles de empresas popularmente conhecidas. Desconfie de muita oferta no caso de aplicações gratuitas, pois alguns serviços não-pagos geralmente oferecem risco maior aos seus equipamentos e até mesmo a sua privacidade e reputação.

Ao navegar em sites pode-se observar algumas imagens instantâneas, que são os pop-ups. Alguns pop-ups podem direcionar ou acionar mecanismo que coloquem seus dados e sua reputação em risco ou sugerem atualização de algum aplicativo ou software de seu equipamento dizendo, que está desatualizado. É comum, ao navegar, aparecer mensagens de prêmios e, ao clicar no link, pode ser uma cilada.

Ser popular demais nas redes sociais também pode ser um grande problema. Em redes sociais, como o Facebook, é comum as pessoas colocarem toda a sua vida, o dia-a-dia, o que fazem, onde moram, onde estudam e o que possuem. Esse é um prato cheio para pessoas que buscam ganho fácil com informações pessoais. Filtre regularmente os contatos existentes em seus sites de relacionamento e confira inteiramente suas configurações de privacidade.

O wi-fi hoje tornou-se mais difundido em estabelecimentos comerciais, como bares e restaurantes, que oferecem navegação em sua rede gratuitamente. Nesses ambientes deve-se ter mais cautela ao inserir dados confidenciais, senhas de bancos

ou conteúdos pessoais, pois podem ser capturados e usados indevidamente. Prefira, nestes casos, utilizar a sua internet, do celular ou modem.

Não armazene senhas no navegador. Lembre-se sempre de executar a limpeza de histórico do seu navegador com frequência.

Ao criar senhas para os mais variados acessos a sites, sistemas e aplicativos, sempre crie senhas que tenham um grau de dificuldade. Utilize letras, números e caracteres especiais, evite utilizar os números de seus documentos, como CPF, e sequências como abcd, 1234, carteira de identidade ou datas de nascimentos, além de manter senhas diferentes para cada software, site ou aplicativo.

Em ambientes de educação tem-se conexões em vários momentos por professores, alunos e funcionários. Dispositivos removíveis como pen drives, CD, DVD, dentre outros devem ser monitorados, pois existem várias ameaças auto-executáveis onde ao conectar na rede cria vínculos não desejados.

O plágio é a prática de diversas áreas e, no ambiente de educação, não é diferente. Usuários fazem o uso de trabalhos e obras intelectuais trazendo para si o mérito da autoria alheia. Isso é crime previsto no Código Penal Brasileiro e se enquadra na modalidade de crimes contra a propriedade intelectual. Cópia de um texto total ou parcial, músicas, vídeos e imagens sem dar os devidos créditos/méritos ao respectivo autor é crime com

pena prevista em lei. Citando os textos ao invés de copiá-los, você só tem a ganhar.

De acordo com o Marco Civil, conheça alguns Direitos e Deveres dos estudantes em relação à tecnologia:

Direitos

- Direito de acesso à informação;
- Direito à tecnologia;
- Direito à educação e oportunidades garantidas pela internet;
- Direito de expressão;
- Direito de emitir opiniões a respeito de assuntos variados;
- Direito à proteção da pessoa humana;
- Direito de não ser discriminado, nem humilhado;
- Direito de se divertir e jogar na internet;
- Direito à intimidade, já que dados pessoais e imagens não podem ser divulgados na internet sem permissão;
- Direito de denunciar violação, discriminação, preconceito, bullying e cyberbullying, dentre outros.

Deveres

- Respeito à lei de direitos autorais (como, por exemplo, não baixar música de ambientes não autorizados, não copiar textos ou imagens sem colocar a devida referência ou autoria, não plagiar);
- Respeito aos direitos humanos (não postar conteúdos que contenham qualquer forma de discriminação, preconceito

religioso, político, racial, social, de gênero, ou violação de direitos da pessoa humana ou que induzam à violência e ao crime);

- Respeito à liberdade de expressão de opiniões (como, por exemplo, não humilhar ou discriminar pessoas em redes sociais em função de divergência de opiniões);
- Respeito à intimidade e à integridade da pessoa humana (Exemplo: não postar fotos ou imagens de cunho sexual ou erótico);
- Respeito ao Estatuto da Criança e do Adolescente, ao Estatuto da Juventude, ao Estatuto do Idoso (não postar fotos ou imagens de pessoas nuas ou seminuas, não postar comentários ou fotografias que humilhem, discriminem ou veiculem violência, exposição de intimidade ou violação da integridade física e psicológica de pessoas);
- Respeito à verdade (não escrever algo que não seja verdadeiro sobre qualquer pessoa);
- Respeito ao Estatuto da Igualdade Racial;
- Respeito ao Marco Civil da Internet.

Redes sociais e uso consciente



As redes sociais são sites para criar páginas pessoais na internet, encontrar amigos, fazer novas amizades, participar de comunidades com ideias em comum, trocar fotos, vídeos, depoimentos, enfim, criar várias redes de conhecimento e relacionamento.

O Facebook, Twiter, Google+ e Instagram são os mais utilizados no Brasil e facilitaram a aproximação de diferentes pessoas e culturas. Porém, podem apresentar perigos a partir da divulgação excessiva de dados e informações pessoais que permitam a identificação de locais onde mora, estuda, frequenta e, principalmente, fotos e vídeos os quais não gostaria que todos

tivessem acesso e pudessem divulgar em grande escala. Uma atenção quanto às configurações de privacidade da rede e à permissão para somente pessoas conhecidas participarem do perfil são cuidados simples que podem impossibilitar exposições desnecessárias, perigos virtuais e constrangimentos.

Após a publicação de algo em uma rede social em que o acesso é liberado a todos, não se tem como voltar atrás. Fotos, vídeos e arquivos podem ser compartilhados, copiados, modificados e repassados de forma inapropriada, o que ocasiona, em muitos casos, constrangimentos e até mesmo cyberbullying.

Essas redes normalmente determinam uma idade mínima para a criação de perfil de usuário, o que nem sempre é respeitado e que caracteriza crime de falsidade ideológica.

Além disso, a exposição ou participação em grupos preconceituosos, violentos ou com objetivos duvidosos podem se caracterizar, também, como crimes ou prejudicar o currículo pessoal, já que esses sites mantêm um histórico de tudo que é postado.

A escola é um ambiente que nos coloca em constante socialização, seja entre colegas, seja com professores. É um ambiente de trabalho e um ambiente de estudo, pesquisa, encontro e vivência. Assim, é um ambiente que requer que sejam observados todos os cuidados de respeito à pessoa humana e aos seus direitos. Assim, recomendamos nos mais diferentes espaços de convivência da escola:

- nunca filme uma pessoa (colega ou professor) ou grave seu depoimento sem prévia autorização;

- nunca poste imagens, vídeos ou depoimentos de pessoas (colega ou professor) sem sua prévia autorização;
- evite comentários ofensivos, preconceituosos ou que induzam à violência em redes sociais e nos círculos de convivência na escola;
- denuncie às autoridades escolares quando você ou um conhecido estiver sofrendo preconceito, bullying, cyberbullying, racismo, incitação à violência e ao ódio, racismo, exposição de intimidade, sexting humilhações em redes sociais e na convivência na escola;
- promova campanhas e participe de ações coletivas na escola e na sociedade que visam conscientizar as pessoas acerca dos seus direitos e das responsabilidades em relação ao uso seguro da internet.

VÍCIO TECNOLÓGICO

O acesso “fácil” a smartphones, lan house, tablet, notebook, netbook, etc. e, principalmente, internet cabeadas ou wi-fi apresenta grande risco para os usuários.

Os casos de acompanhamento de pessoas de todas as idades que estão se tornando “viciados tecnológicos” cresce cada vez mais apresentando, como consequência, grandes perdas de rendimento escolar, profissional, comprometimento da personalidade (danos emocionais e psicológicos) e um contínuo aumento dos índices de acidentes.

Sinais de alarme

- Ficar boa parte do dia ao computador e não se interessar por outras atividades em casa, na escola ou no convívio social;
- Ficar constantemente acessando o celular para acompanhar as alterações nas redes sociais e bate papos, não se preocupando com o local e horário mais apropriado para essa atividade.

- Ficar muito tempo online ao invés de socializar com amigos ou familiares, inclusive preferir fazer suas refeições na frente da televisão ou computador;
- Sentir obrigação constante de estar online ou de compartilhar tudo o que faz;
- Não dormir ou continuar até tarde da noite jogando ou navegando na internet;
- Acordar durante a noite para acessar as redes sociais;
- Apresentar ansiedade e nervosismo se ficar algum tempo sem jogar ou estar online.

O que fazer?

Ao identificar estes comportamentos é importante procurar ajuda com profissional especializado, já que esse vício deve ser abordado como qualquer outro vício, como: abuso de álcool e drogas. Ele prejudica drasticamente o desenvolvimento e a saúde física, mental e social.

Dicas

- Reduzir o uso de jogos, redes sociais e bate papo, determinando o tempo mais adequado para o seu uso e acesso;
- Controlar o abuso da tecnologia. Evitar mantê-la muito próxima e sempre à mão;
- Substituir o uso constante por socialização com pessoas, como sair com os amigos, estudar, etc.

Ciberbullying e Sexting



Internet conquistou o mundo. Rompeu fronteiras, diminuiu distâncias. Tornou-se uma constante em nossa vida, graças aos inúmeros aplicativos que trazem facilidade de comunicação, rapidez na transmissão das informações, entretenimento, interação social e muitos outros atrativos, seduzindo principalmente, crianças, adolescentes e jovens.

Um ciberespaço é um ambiente público e livre, infelizmente inseguro. No mundo real existem muitas práticas ilegais e criminosas na rede, criando situações de perigo e risco para os internautas. Um exemplo é o bullying praticado no mundo virtual: o ciberbullying, que usa da tecnologia para humilhar, hostilizar e ofender uma pessoa. As publicações ofensivas se espalham

rapidamente, tornando muito difícil removê-las completamente da rede, ou seja, perde-se o controle da foto, vídeo ou texto postado. Como consequência, os insultos tornam-se repetitivos. A vítima se sente intimidada e perseguida, abandonando o convívio social. Este tipo de agressão virtual pode causar sérios danos emocionais e psicológicos.

Atualmente, uma nova forma de ciberbullying tem preocupado ainda mais pais e professores, pois se torna cada vez mais rotineiro entre os jovens: o sexting, que consiste em produzir e publicar imagens sensuais do próprio corpo (seminu ou nu), utilizando celulares, redes sociais e webcam. Esta exposição é muito arriscada, já que, ao cair na rede, qualquer pessoa no mundo pode visualizar, copiar e até modificar as imagens postadas. Para os jovens, o sexting é uma forma de “status” e expressão da sexualidade mas, para pessoas mal intencionadas, é uma oportunidade para cometer práticas ilegais e invadir a privacidade alheia.

Para evitar estes crimes virtuais é muito importante o papel da escola e dos pais. Um trabalho em parceria proporciona a redução destes casos.

A escola deve realizar ações preventivas, conscientizando os estudantes quanto ao uso da internet e seus perigos, destacando noções de privacidade, direitos humanos, segurança e legislação sobre crimes virtuais, assim como instruir os pais a ficarem atentos sobre o que os filhos fazem na internet.

Aos pais cabe a responsabilidade sobre o comportamento dos filhos na internet. Portanto, é importante saber a que páginas acessam, quem são suas amizades virtuais, o que postam nas redes sociais, etc. Em caso de crimes virtuais, como o cyberbullying, os pais podem ser responsabilizados e processados dos atos praticados pelos filhos. O melhor caminho não é a punição ou a proibição, mas a educação preventiva, que prepara e orienta quanto a navegar com segurança, cidadania e respeito a todos.

Os estudantes devem observar que qualquer publicação na rede pode ter consequências dentro e fora da internet, inclusive criminais. A privacidade deve ser respeitada. Assim, não poste nada que cause constrangimento a si ou a terceiros nem participe de comunidades ou grupos que são adeptos a causas violentas, raciais ou pornográficas. Cuidado com seus dados pessoais, de familiares ou amigos, informados na rede.

Um internauta consciente navega com responsabilidade, cautela e respeito ao outro. O futuro de uma internet justa e segura está em suas mãos!

Privacidade e Aliciamento



Privacidade

Quando postamos nossas imagens e dados pessoais na internet, pessoas do mundo todo podem ter acesso às informações. Consequentemente, essas informações poderão ser usadas para vários fins, inclusive ilícitos.

Com a assinatura do Marco Civil da Internet em 2014, o Brasil passou a regulamentar os direitos e deveres para o uso da Internet no Brasil. Conforme o Marco Civil da Internet, art. 10º da Lei nº 12.965, de 23 de abril de 2014:

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como

de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. (BRASIL, 2014)

Apesar de o Brasil possuir uma lei de proteção à privacidade é importante que façamos nossa parte. Pense antes de postar! Preserve sua privacidade! Pois nem tudo deve ser exposto na internet.

Como podemos proteger nossos dados pessoais?

De acordo com a Central de Proteção e Segurança da Microsoft devemos seguir as seguintes recomendações:

- Pense antes de compartilhar informações pessoais;
- Leia a política de privacidade do site;
- Não revele mais informações do que o necessário;
- Não publique nada online que você não gostaria que se tornasse público;
- Minimize detalhes que o identifiquem ou que identifiquem sua localização;
- Mantenha segredo de números de telefone, contas, nomes de usuários e senhas.
- Insira somente as informações necessárias marcadas com asterisco (*) nos sites;
- Crie senhas seguras;
- Não utilize a mesma senha em todos os sites;
- Monitore o que postam sobre você na internet;
- Somente faça operações bancárias ou confidenciais em seu computador;
- Tenha o antivírus atualizado;

- Desconfie de negócios que pareçam “bons demais para ser verdade”, anúncios falsos de emprego, avisos de que você ganhou na loteria, solicitações para ajudar um estranho, dentre outros.
- Desconfie de mensagens urgentes (“Sua conta será fechada!”).

Aliciamento (Megaexposição, falsas promessas, chantagem online e vazamento de informações)

O aliciamento pode acontecer quando uma pessoa adulta tenta seduzir, convencer e chantagear crianças ou adolescentes com o objetivo de marcar encontros, produzir imagens eróticas, sexuais e cometer abuso sexual infanto-juvenil online ou offline. Muitas vezes esses adultos se disfarçam como crianças ou adolescentes, com o intuito de conseguir imagens sexuais, para venda ou para uso próprio. Isso pode acontecer em salas de bate-papo, redes sociais e chats instantâneos, como: o WhatsApp, etc.

Quais os cuidados para evitar o aliciamento?

- Não aceitar o contato de usuários desconhecidos que tentam se aproximar em salas de bate-papo, redes sociais, chats instantâneos;
- Não fornecer informações sobre você, seus amigos e familiares;
- Nunca enviar fotos ou utilizar a webcam com pessoas desconhecidas;
- Não se sentir pressionado a agradar pessoas, enviando informações pessoais e imagens;
- Pedir a ajuda de um adulto de confiança;
- Denunciar qualquer ato de megaexposição ou aliciamento nos canais que constam nessa cartilha.

O uso dos celulares nas escolas: Vilão ou Aliado?



De modo geral, este assunto é polêmico, mas muito importante, pois o “celular” pode ser um grande colaborador do ambiente educativo.

O que acontece, muitas vezes, é que ele acaba por se tornar um dificultador, se não utilizado corretamente, gerando falta de limites e podendo comprometer o rendimento dos alunos.

A utilização de dispositivos móveis em sala de aula, e na escola entretanto, como celulares, smartphones, laptops e tablets, por exemplo, não pode ser encarada como vilão da história.

De vilão, o celular deve ser um apoio, uma vez que é interessante e pode trazer uma transformação positiva à Educação.

Não basta simplesmente negar ou punir em relação ao uso destes dispositivos. Pode-se criar estratégias motivacionais e pedagógicas de uso consciente, criativo, adequado e seguro.

A inclusão do celular no cotidiano escolar precisa acontecer junto com o processo das diferentes tecnologias, colaborando com o processo ensino-aprendizagem, para o estabelecimento de uma nova Cultura Digital na Escola.

Não há como dissociar a educação da ciência, tecnologia e inovação, assim como não se falar em modernidade sem se retratar a rotina humana.

Este trabalho precisa ser perseverante, de modo continuado e progressivo, e ter um caráter formador e interativo.

Deste modo, o uso pedagógico das novas mídias digitais deve ser defendido e priorizado, a fim de garantir modernidade e atender às expectativas de uma escola ética, cidadã e inclusiva digitalmente, dinamizando seu espaço.

Um pensamento para refletir, é: Como usar esta tecnologia a favor da Educação?

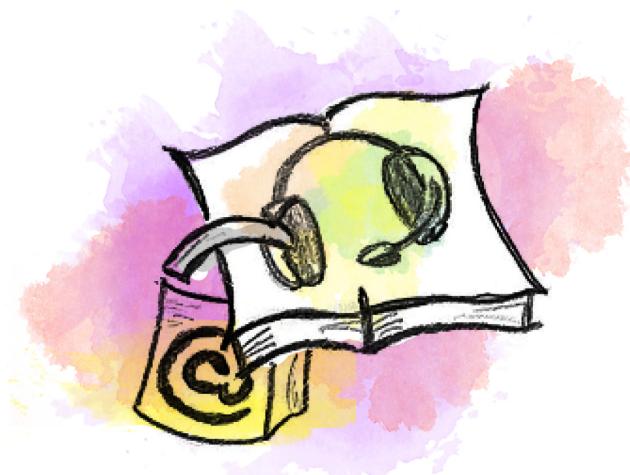
Os telefones celulares mesmo os mais simples, por exemplo, possuem mecanismos facilitadores do processo ensino-aprendizagem. Vejamos alguns deles:

- realizam interações por meio de voz, player, gravador, transmissão de rádio, fotografam, filmam, etc;
- transmitem torpedos, têm calculadora, bloco de notas, ajuste de fuso-horário, alarme, cronômetro, conversão de moedas, agenda, calendário, lembretes de tarefas, alteração de layouts, dentre outros;
- professores e alunos podem compartilhar materiais, dicas de sites e muito mais, como: webquest, quiz;
- por meio de um smartphone ou tablet os alunos podem desenvolver mídias, o que permite que eles estudem e socializem saberes;
- os aplicativos diversos têm recursos diferenciados, como: e-books, músicas, filmes, jogos, chats e muito mais, podendo ser um complemento de outros materiais utilizado na aprendizagem;
- ótima ferramenta de incentivo de participação em sala ampliando a discussão para pós-aula, por meio das redes sociais, interação nos fóruns e grupos criados para tal.

Portanto, o “mobile learning” ou “m-learning” pode ser adotado e difundido mas, a criação de medidas motivacionais, conscientizadoras, educativas (preventivas, de monitoramento e de intervenção), precisam ser estabelecidas para garantir o uso que os alunos já fazem destas mídias no seu dia-a-dia seja de forma direcionada e não dispersiva em sala de aula (e fora dela).

Estabelecer um acordo de uso responsável com os alunos, no qual o processo educativo transcorra com segurança, criatividade, responsabilidade e competência, de modo adequado e otimizado, faz deste uso tecnológico um **aliado à Educação**.

Canais de Denúncia



Segue a lista dos principais canais de denúncia e orientações quanto a crime virtual:

E-mails:

- mail-abuse@cert.br: para encaminhamento de denúncias de mensagens fraudulentas.
- phishing@cais.rnp.br: para encaminhamento de denúncias mensagens fraudulentas.
- artefatos@cais.rnp.br: para encaminhamento de denúncias de aplicativos suspeitos.

Sites:

- **Humanize Redes** - denúncias de mensagens preconceituosas, racistas, xenófobas e que violem os Direitos Humanos.
- **Digi Denúncias** - canal para denúncias de crimes eletrônicos do Ministério Público.
- **Safernet** - denúncias de crimes como Pornografia Infantil, Racismo, Xenofobia e Intolerância religiosa, Neonazismo, Apologia e Incitação a crimes contra a Vida, Homofobia, Apologia e Incitação a práticas cruéis contra animais e tráfico de pessoas.
- **ic3.gov** - denúncias de crimes digitais internacionais.

Referências

Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco Civil da Internet. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato20112014/2014/Lei/L12965.htm>. Acesso em: 11 nov. de 2015.

CUNHA, Juliana Andrade; NEJM, Rodrigo. *Diálogo Virtual 2.0* preocupado com o que acontece na internet? Quer conversar? 4. ed. Salvador: Safer-Net Brasil, 2015.

MICROSOFT. Central de Segurança. Disponível em: <<https://www.microsoft.com/pt-br/security/online-privacy/prevent.aspx>>. Acesso em: 11 nov. de 2015.

Direitos e deveres na internet <https://www.oficinadanet.com.br/artigo/internet/direitos-e-deveres-na-internet>. Acesso em: 11 nov. de 2015.

Internet. O maior espaço público na história da humanidade. <http://porvir.org/7-dicas-para-falar-de-internet-segura-na-escola/> . Acesso em: 11 nov. de 2015.

Internet como expressão e extensão do espaço público

www.matrizes.usp.br/index.php/matrizes/article/download/102/162
. Acesso em: 11 nov. de 2015.

Como denunciar crimes virtuais <http://www.crimespelainternet.com.br/como-denunciar-crimes-digitais/> Acesso em: 11 nov. de 2015.

GUIA DA UNESCO: Guia de Tecnologias Educacional e documento afim, como "Diretrizes de Políticas para a aprendizagem móvel" ("Policy guideline for mobile learning"), com recomendações e motivos para usar os celulares como recurso educacional foi lançado pela Unesco. <http://unesdoc>



SECRETARIA DE
EDUCAÇÃO

