

Guia de Conduta Ética e Segurança Digital

Para Corpo Docente e Colaboradores

INTRODUÇÃO

As Escolas/Colégios da IMACULADA REDE DE EDUCAÇÃO são voltados para a educação de jovens na Educação Infantil, Ensino Fundamental e Médio com o objetivo de alcançar o pleno desenvolvimento de seus alunos, prepará-los para o exercício da cidadania e qualificá-los para o mercado de trabalho, por meio de atividades construídas sobre os princípios da igualdade, liberdade de aprender e ensinar, pluralismo de ideias, aceitação, ética, comprometimento, sustentabilidade, respeito, transparência, trabalho em equipe, honestidade, valorização do profissional da educação e responsabilidade social, ambiental e digital.

Para alcançar esses objetivos, atendendo aos princípios mencionados, **colaboradores e docentes precisam estar alinhados com a nova realidade da Sociedade Digital** na condução das atividades profissionais e educacionais, e na utilização das informações e dos Recursos Educacionais de Tecnologia da Informação e Comunicação (RETIC).

A mobilidade e a ausência de perímetros físicos e fronteiras claras da sociedade digital, permitida pelos avanços tecnológicos, exige muito mais cuidado para evitar incidentes que possam colocar em risco a Escola, seus colaboradores, docentes e alunos, e que podem trazer impactos negativos ao objetivo educacional, sua imagem e reputação.

Nesse contexto, a **ética e a segurança digital** são princípios essenciais para a proteção de todos os ativos tangíveis e intangíveis da Escola, a exemplo de imagem, reputação, conhecimento, patrimônio e a própria informação. Desse modo, é fundamental que todos os integrantes da IMACULADA REDE DE EDUCAÇÃO, seja na área administrativa ou nos núcleos de docentes ou de discentes, pratiquem e disseminem os princípios da **ética e da segurança digital**.

O sucesso deste **Guia de Conduta Ética e Segurança Digital** depende da combinação de requisitos das atividades da Escola, de estrutura de processos, do uso de tecnologias e mecanismos de proteção e, o mais relevante, **o comportamento dos colaboradores independentemente do nível hierárquico e da atividade desenvolvida para a Escola, seja ela administrativa ou educacional**.

Por isso, é papel de cada integrante da comunidade escolar proteger a informação, principalmente a de nossos alunos, bem como todos os ativos intangíveis e RETICs da IMACULADA REDE DE EDUCAÇÃO **por meio da aplicação de todas as diretrizes presentes neste Guia** e da disseminação do uso ético, seguro, responsável e legal da tecnologia e da informação por toda a Escola, inclusive pelos alunos, seus pais e responsáveis legais.

OBJETIVO

1.1. Este Guia é aplicável ao ambiente educacional e administrativo tem por objetivo:

1.1.1. Nortear a tomada de decisão e a realização das atividades profissionais e educacionais, independente se em ambientes presenciais ou digitais, sempre de acordo com os normativos da Escola, a ética, a moral e a legislação nacional vigente.

1.1.2. Declarar o apoio da Escola para a segurança da informação de acordo com os requisitos da atividade da IMACULADA REDE DE EDUCAÇÃO e com as leis e regulamentações pertinentes.

1.1.3. Estabelecer os princípios para o desenvolvimento de uma atividade estudantil/acadêmica ética, responsável, segura e legal, que afaste danos para a reputação da IMACULADA REDE DE EDUCAÇÃO, de seu corpo docente e discente.

1.1.4. Zelar por **relações transparentes, responsáveis e éticas**, e promover o uso lícito e adequado dos conteúdos e recursos educacionais.

1.1.5. Zelar pela proteção do ambiente de trabalho e dos RETICs disponíveis, sejam eles institucionais e/ou particulares.

ABRANGÊNCIA

1.2. Este Guia foi aprovado e publicado pela IMACULADA REDE DE EDUCAÇÃO e será aplicado em todas as Escolas/Colégios, abrangendo docentes e colaboradores administrativos, inclusive equipes terceirizadas e prestadores de serviços.

SEGURANÇA DA INFORMAÇÃO

1.3. Segurança da Informação significa a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação, com o objetivo de proteger os ativos tangíveis e intangíveis da IMACULADA REDE DE EDUCAÇÃO, inclusive a sua imagem e reputação.

PRINCÍPIOS GERAIS

1.4. Educar pelo exemplo com a prática de ações pautadas pela ética, segurança e legalidade no ambiente escolar, em atenção aos princípios da igualdade, liberdade de aprender e ensinar, pluralismo de ideias, aceitação, comprometimento, honestidade, sustentabilidade e respeito mútuo.

1.5. Promover o aprendizado por meio do uso ético, seguro e legal da tecnologia no ambiente educacional, para facilitar e melhorar a aprendizagem, bem como evitar qualquer distração ou dispersão.

1.6. Disseminar em toda a comunidade escolar os princípios da boa-fé, da moral e dos bons costumes.

1.7. Respeitar a privacidade, a liberdade de expressão, o direito de imagem, os direitos autorais e os seus limites estabelecidos pela legislação vigente no Brasil.

1.8. Fazer o uso ético, responsável e seguro dos RETICs (institucionais ou particulares) e das informações da Escola, especialmente a dos alunos, a fim de garantir a proteção e a preservação do conteúdo criado, recebido, mantido, armazenado ou sob responsabilidade da IMACULADA REDE DE EDUCAÇÃO.

1.9. Respeitar a Proposta Pedagógica e os valores educacionais da IMACULADA REDE DE EDUCAÇÃO, para proteção da imagem, reputação e identidade da Escola, de seus colaboradores, docentes, alunos e toda comunidade escolar.

1.10. Respeitar o Estatuto da Criança e do Adolescente, a Lei de Diretrizes e Bases da Educação Nacional e a legislação vigente do Brasil.

MELHORES PRÁTICAS DE ÉTICA E SEGURANÇA DIGITAL

1.11. Proteger a identidade digital, que pode ser composta por crachá, senha, *token*, biometria ou outros recursos de autenticação, devendo ser utilizada de forma individual e exclusiva, não compartilhando, divulgando ou transferindo a terceiros em hipótese alguma.

1.12. Proteger as informações sigilosas, críticas e/ou sensíveis, que digam respeito a dados pessoais de alunos e seus familiares, contra o acesso de pessoas não autorizadas ou alheias à comunidade escolar.

1.13. Manter sempre habilitados e atualizados softwares de proteção e segurança em RETICs institucionais e/ou particulares.

1.14. Utilizar somente softwares legítimos e previamente autorizados em RETICs institucionais, respeitando os direitos de propriedade intelectual da IMACULADA REDE DE EDUCAÇÃO e de terceiros.

1.15. Utilizar linguagem adequada e compatível com o ambiente educacional, evitando-se termos que possam denotar excesso de intimidade, perseguição, violência, agressão, discriminação ou algum tipo de assédio moral ou sexual ou mesmo expor a intimidade do docente, do aluno, colaboradores ou prestadores de serviços.

O QUE EVITAR

1.16. Captar ou reproduzir quaisquer imagens, vídeos ou sons, de dentro de perímetro físico da Escola, de seus colaboradores, docentes e/ou alunos, bem como para compartilhar este conteúdo com terceiros ou via Internet, mídias sociais e aplicativos de comunicação, sem a expressa autorização prévia da Direção.

1.17. Excessos de exposição em ambientes sociais, sejam presenciais ou digitais, a exemplo da Internet, e-mails e mídias sociais. Recomendamos evitar comentários sobre rotinas, problemas e opiniões pessoais que possam ser confundidas com a posição oficial da Escola ou a seu respeito, ou que possam comprometer a sua imagem e reputação, a da Escola ou dos alunos e demais colaboradores.

1.18. Abrir e-mails, links e arquivos que possam ter conteúdo com vírus, arquivo malicioso ou mesmo de conteúdo duvidoso, sem a devida verificação prévia por aplicativos de proteção e segurança.

1.19. Fazer o uso dos RETICs da Escola para acessar, baixar, utilizar, armazenar ou divulgar qualquer conteúdo ilícito, impróprio, obsceno, pornográfico, difamatório, discriminatório, que atente à moral, à ética ou aos bons costumes, que viole a boa-fé, que prejudique a harmonia do ambiente escolar, tenha teor agressivo ou que não seja compatível com o propósito educacional e as diretrizes da IMACULADA REDE DE EDUCAÇÃO.

1.20. Deixar papéis e RETICs expostos em mesas de trabalho, *flipcharts*, impressoras, fax, *scanner*, salas de aula, pátios, telas de computadores, áreas comuns, locais de trânsito de pessoas, elevador, refeitório e nas salas de reunião, principalmente quando não estiverem sendo utilizados.

1.21. Deixar de bloquear o RETIC que estiver em posse com senha ao se distanciar, seja a estação de trabalho ou o dispositivo móvel, inclusive quando estiver ou permanecer na sala de aula.

1.22. Qualquer prática ou método para burlar as restrições ou alterar as permissões aplicadas aos RETICs institucionais.

1.23. Utilizar a marca da IMACULADA REDE DE EDUCAÇÃO, sem prévia e expressa autorização, inclusive para criação de perfis em mídias sociais em nome da Escola e/ou se fazendo passar por ela.

1.24. Utilizar correio eletrônico particular ou público, como Gmail ou Hotmail, serviços e aplicativos de armazenamento da nuvem, comunicadores instantâneos e/ou aplicativos sociais e de comunicação **para a transmissão de conteúdos e informações sigilosas, críticas e/ou sensíveis de propriedade da Escola ou**

sob sua responsabilidade. Excepcionalmente, na hipótese desta prática ser necessária e justificável, sujeita à aprovação de responsável imediato, sempre aplicar as medidas de segurança digital recomendadas por este Guia.

2. DEVER DE VIGILÂNCIA

2.1. Os colaboradores e docentes estão cientes, por seu livre consentimento expresso, das práticas de monitoramento e inspeção que a IMACULADA REDE DE EDUCAÇÃO, **realiza, com o registro e armazenamento de atividades (logs) e o monitoramento de todos os seus ambientes físicos e lógicos**, com a captura de imagens, áudio ou vídeo, inclusive, com a finalidade de proteção de seu patrimônio e reputação e daqueles com os quais se relaciona de alguma forma e, portanto, desde já, comprometem-se a colaborar, proativamente, com os procedimentos de segurança e vigilância, sempre que necessário ou que lhe seja solicitado.

2.2. A IMACULADA REDE DE EDUCAÇÃO **realiza o armazenamento dos dados monitorados** para fins administrativos e legais, além de colaborar com as autoridades em caso de investigação.

2.3. A IMACULADA REDE DE EDUCAÇÃO pode realizar, quando necessário, de forma proporcional e dentro dos limites da razoabilidade, da ética e da proporcionalidade, **eventual revista e/ou inspeção em dispositivos próprios, particulares ou de terceiros**, para finalidade de segurança da própria comunidade Escolar, nos limites do interesse público e da legítima defesa que cabe à Instituição, respeitando a privacidade do proprietário do dispositivo e a proteção de seus dados pessoais, sempre em conjunto com a Coordenação, Direção e/ou do departamento de Tecnologia da Informação (TI), e com o acompanhamento do detentor e/ou proprietário do dispositivo.

3. INCIDENTES

3.1. Todos os incidentes que possam impactar na segurança das informações da IMACULADA REDE DE EDUCAÇÃO **devem ser imediatamente reportados à Direção da Escola pelo e-mail direção@ensa.org.br**

3.2. Uma vez informada, a Direção levará o caso para a área de Tecnologia de Informação e/ou outra área responsável, que agirá de forma remediativa e imediata, para eliminar ou mitigar o que deu causa ao incidente, bem como fazer a adequada preservação de evidências para fins de eventuais medidas disciplinares, administrativas e legais que devam ser aplicadas.

3.3. Mediado e contido o incidente em caráter emergencial, a Direção poderá oportunamente levar o caso para apreciação e envolvimento de outras áreas para tomada das medidas cabíveis, inclusive para análise de ações preventivas que possam ser aplicadas para evitar nova ocorrência.

4. COMPROMISSO COM A EDUCAÇÃO

4.1. A IMACULADA REDE DE EDUCAÇÃO está comprometida com o dever de capacitar constantemente seus colaboradores e docentes no uso ético, seguro e legal das informações e da tecnologia, por isso, realiza programas de educação em segurança da informação para aumentar o nível de cultura em segurança digital na Instituição.

5. RECOMENDAÇÕES PARA OS COLABORADORES E DOCENTES

5.1. Todos os ativos intangíveis, RETICs institucionais e informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao colaborador/docente ou das quais tiver acesso no exercício de suas atividades, **são de propriedade da IMACULADA REDE DE EDUCAÇÃO ou estão a ela cedidos.**

5.2. Todas as informações e RETIC da IMACULADA REDE DE EDUCAÇÃO devem ser utilizados **apenas para o cumprimento das atividades profissionais e educacionais, limitados à função do colaborador/docente, dentro do padrão de conduta ética e moral estabelecida pela Escola.**

5.3. **Os colaboradores e docentes precisam sempre utilizar trajés adequados** aos ambientes de trabalho e educacional.

5.4. Para que as informações sejam adequadamente protegidas, cabe ao colaborador/docente realizar a classificação no momento em que ela for obtida ou gerada, por ele ou por terceiros, para garantir a devida confidencialidade, além de cumprir com a classificação estabelecida pela IMACULADA REDE DE EDUCAÇÃO.

5.4.1. Informações sigilosas, críticas e/ou sensíveis para o exercício das atividades educacionais (provas - aplicadas ou não, plano pedagógico detalhado, etc.), ou protegidas legalmente (como prontuário de informações pessoais de alunos), em posse da IMACULADA REDE DE EDUCAÇÃO devem ser consideradas sigilosas e receberem o rótulo de **confidenciais**. Cabendo somente acesso previamente autorizado e não são passíveis de publicação, divulgação ou compartilhamento com terceiros ou em ambientes externos à Escola, incluindo Internet e mídias sociais, salvo sob autorização prévia e expressa da Direção.

5.4.2. Informações relacionadas com as atividades profissionais e educacionais (como modelos de contratos e sumários do plano pedagógico) da IMACULADA REDE DE EDUCAÇÃO, que não possuem grande criticidade ou proteção legal, são consideradas de **uso interno**. Podendo ser compartilhadas com alunos, pais e/ou responsáveis legais, colaboradores e docentes.

5.4.2.1. O uso interno alcança os recursos de compartilhamento de conteúdo autorizados pela Escola para acesso apenas aos seus integrantes como a rede, a Intranet, o Portal Escolar e os perfis institucionais da IMACULADA REDE DE EDUCAÇÃO em mídias sociais. Porém, não são passíveis de publicação, divulgação ou compartilhamento com terceiros alheios às atividades da IMACULADA REDE DE EDUCAÇÃO ou em ambientes externos à Escola, incluindo páginas de Internet e perfis de mídias sociais fora os da própria Escola, sem prévia autorização da Direção.

5.4.3. Informações que foram criadas com o propósito de divulgação e publicação geral sobre atividades da IMACULADA REDE DE EDUCAÇÃO são consideradas de **uso público** e podem ser compartilhadas em qualquer meio, ambiente ou suporte, para qualquer pessoa.

5.4.4. Em caso de dúvida, recomendamos que o colaborador ou docente trate a informação como de uso confidencial ou consulte pontualmente a Direção.

5.5. A IMACULADA REDE DE EDUCAÇÃO controla o acesso físico e lógico aos seus ambientes e RETICs, para tanto, é fornecida ao colaborador/docente uma **identidade digital** de uso individual e intransferível, podendo abranger crachá, *login*, senha, *token*, certificado digital e outros recursos que venham a ser implantados.

5.5.1. O colaborador/docente é responsável pelo **uso e o sigilo de sua identidade digital**, e não é permitido fazer o seu uso não autorizado, compartilhar, divulgar ou transferir a terceiros.

5.5.2. Todo colaborador e docente devem passar pelos controles de entrada e saída da IMACULADA REDE DE EDUCAÇÃO, **usando carteiras ou crachás de identificação para obtenção do acesso.**

5.6. A mera possibilidade de acesso aos ambientes lógicos da Escola, às suas informações, o porte ou uso de qualquer dispositivo móvel para finalidade profissional e/ou educacional (RETICs), inclusive de forma remota, bem como as interações com alunos, pais e/ou responsáveis legais através de mídias sociais ou outros meios digitais, fora do horário do expediente normal da Escola, por ser intrínseco ao relacionamento estabelecido ou por ser da própria conveniência ou liberalidade do colaborador, por si só, não implicará em requisição de trabalho, sobrejornada, sobreaviso ou plantão, e nem ensejará prejuízo à vida social, ao lazer ou seu descanso, pois os dados e recursos permanecem ativos ou disponíveis independentemente de sua vontade ou comando ou requisição da Escola.

10.6.1. As atividades desempenhadas fora do expediente dependerão de prévia e expressa requisição de trabalho formal em registros adequados, para serem remuneradas ou compensadas.

10.7. A IMACULADA REDE DE EDUCAÇÃO recomenda que os colaboradores e docentes evitem adicionar alunos em perfis pessoais nas mídias sociais, pois isso pode gerar confusão no ambiente escolar e pode ocasionar excesso de intimidade. Para tanto recomenda-se a criação de perfil específico educacional ou o uso dos canais oficiais da Escola, inclusive das mídias sociais educacionais.

10.8. Os colaboradores e docentes devem manter todas as informações ou conteúdos criados ou recebidos em razão das suas atividades para a IMACULADA REDE DE EDUCAÇÃO armazenados na rede institucional ou, quando físicas, guardadas em gavetas ou armários trancados, quando não estiverem sendo utilizados, principalmente quando envolver documentação de identificação de aluno, provas ou trabalhos educacionais.

10.9. As **informações sigilosas, críticas e/ou sensíveis**, assim como os RETICs, mídias e outros suportes que as contenham, quando descartados, devem passar por procedimento de destruição que impossibilite sua recuperação e o acesso às informações armazenadas por pessoas não autorizadas. Em caso de dúvida, a área de Tecnologia da Informação deve ser consultada acerca do melhor procedimento para realização do descarte seguro.

10.10. A IMACULADA REDE DE EDUCAÇÃO recomenda que os docentes e colaboradores tenham cautela ao acessar softwares, informações e conteúdos disponibilizados gratuitamente na Internet, a exemplo de aplicativos, músicas, vídeos, trabalhos completos, digitalizações de livros físicos e e-mails com propostas suspeitas, pois podem ser vetores de ataques de criminosos como o uso de engenharia social.

10.11. Todos os colaboradores e docentes têm o dever de se manterem atualizados sobre as regras vigentes da IMACULADA REDE DE EDUCAÇÃO e sobre as melhores práticas de segurança da informação, bem como de dar o exemplo, orientar e educar os alunos.

6. RECOMENDAÇÕES PARA OS DOCENTES

11.1 Todo conteúdo de conhecimento próprio ou de terceiros, independente do suporte ou formato, utilizado em aulas e demais atividades de ensino deve mencionar fonte e autoria no padrão determinado pela Associação Brasileira de Normas Técnicas (ABNT), que exige citação de nome de Autor (ou menção à autoria desconhecida), nome da fonte, edição, página e/ou endereço eletrônico quando houver (link), ano de publicação ou data e horário de acesso (se aplicável) e referência ao termo “uso educacional”, quer seja no formato público ou

protegido, aberto ou licenciado, além de respeitar as leis, tratados e convenções internacionais sobre direitos autorais.

11.2. Todo conteúdo criado pela equipe pedagógica no exercício de suas atividades é:

11.2.1. De propriedade da IMACULADA REDE DE EDUCAÇÃO, independente se sua elaboração se deu em RETIC institucional ou particular.

11.2.2. Considerado de uso interno, só podendo ser tornado público para terceiros se previamente autorizado pela Direção.

11.3 Todas as informações criadas ou recebidas por um membro da equipe pedagógica ou administrativa **sobre um aluno** devem ser tratadas com classificação de informação confidencial e só diz respeito à Escola, ao aluno e aos seus pais e/ou responsáveis legais.

11.3.1 A disponibilização dessas informações a terceiros só será feita com a autorização prévia e expressa da Direção, e sem a identificação e individualização do aluno, a não ser em hipótese em que isso se faça necessário com a prévia ciência dos pais e/ou responsável legal.

11.4. A equipe pedagógica deve orientar os alunos a respeitar os direitos de autor na execução de trabalhos, projetos, tarefas, apresentações e outras atividades curriculares e extracurriculares desenvolvidas pela ou para a Escola.

11.4.1. O conteúdo criado por alunos em suas atividades curriculares e extracurriculares:

11.4.1.1. É considerado de uso interno, não passível de divulgação ou publicação do teor do mesmo em ambientes externos aos educacionais (fora da rede, intranet, portal escolar, fanpage ou perfil institucional oficial de ensino), sem a prévia autorização da Escola, independente se sua elaboração se deu em RETIC institucional ou particular, desde que tenha envolvido realização de trabalho escolar;

11.4.1.2. A publicação desse conteúdo em outros ambientes ou plataformas somente deve ocorrer quando a mesma tiver sido considerada na solicitação do trabalho como forma de aprendizagem colaborativa ou como forma de aplicação de ferramentas públicas, de modo a evitar qualquer tipo de exposição indevida de alunos que possa de algum modo descumprir com a lei brasileira;

11.4.1.3. Em atenção ao artigo 17 do Estatuto da Criança e do Adolescente, o docente e/ou o colaborador não estão autorizados a

publicar abertamente na Internet ou nas mídias sociais externas aos ambientes da escola, mesmo que em seus perfis pessoais, as provas dos alunos, independente da sua identificação ou não;

11.4.1.4. IMACULADA REDE DE EDUCAÇÃO poderá fazer uso de ferramentas para a detecção de plágio nos trabalhos estudantis;

11.4.1.5. Poderá ser usado como referência para trabalhos e discussões posteriores da equipe pedagógica.

11.5. Os membros da equipe pedagógica farão uso do Portal Escolar para disponibilizar informações, documentos, recursos educacionais e outros materiais, de sua elaboração ou de terceiros, para alunos e membros da comunidade escolar, observando sempre as regras aplicáveis de direitos autorais e de direitos de imagem, o decoro, seu sigilo profissional e a postura adequada de sua atividade e função junto à Escola.

11.6. Os usos de RETICs em sala de aula, para fins educacionais, sejam institucionais ou particulares, pelos docentes ou coordenadores pedagógicos só são permitidos quando previsto no plano de aula e presente na proposta da atividade que será realizada.

11.7. Recomendamos que o docente ou outro membro da equipe pedagógica, durante o uso de RETICs no laboratório de informática pelos alunos, tenha atenção e cautela para garantir que os recursos sejam utilizados somente para o desempenho da atividade proposta, e para evitar que não seja praticado ato antiético, ilícito ou infracional, que possa atentar contra a moral e os bons costumes ou ser não compatível com a idade do aluno.

11.8. Ao desempenhar atividades em sala de aula, a equipe pedagógica deve se ater ao plano de aula elaborado em conjunto com Coordenação Pedagógica e responder os questionamentos dos alunos relativos ao tema.

11.8.1. Não devem ser levantadas ou expostas questões de outros colaboradores, docentes ou alunos, ou de assuntos alheios ao tema proposto em aula.

11.8.2. Caso surja a necessidade de esclarecer algum incidente, isso será feito pela Coordenação Pedagógica em conjunto com os envolvidos, dentro das dependências da Escola e com registro documental dos fatos nos ambientes institucionais autorizados. É vedada a exposição dos incidentes na Internet ou nas mídias sociais, ou para terceiros independentemente do meio ou veículo.

11.9. Recomendamos que colaboradores, educadores, membros da equipe pedagógica, dentro e fora da Escola, mantenham sempre uma postura profissional

compatível com o ambiente educacional, e tratem de assuntos com alunos de forma clara e educativa, evitando tópicos que extrapolem os assuntos escolares e/ou de sala de aula ou que possam envolver a vida íntima e/ou pessoal.

11.10. Recomendamos o uso de **linguagem adequada ao ambiente educacional**, sem o uso de termos que possam denotar excesso de intimidade, perseguição, discriminação ou algum tipo de assédio moral ou sexual ou mesmo expor a intimidade do docente/discente.

11.11. Os membros da equipe pedagógica envidarão os melhores esforços para criar uma cultura de práticas éticas, seguras e legais no uso de RETIC e manipulação de informação pelos alunos. O compromisso da Escola é com a formação do indivíduo e a melhor forma de aprender é usando a tecnologia com a devida orientação, vigilância e supervisão, por parte da IMACULADA REDE DE EDUCAÇÃO e da própria família.

11.12. Caso o aluno viole ou tente burlar alguma das determinações do Regimento Escolar, do contrato de prestação de serviços educacionais, das normas e procedimentos escolares, aja de forma antiética, ou cometa atos ilícitos ou infracionais, os membros da equipe pedagógica têm autorização e poderes para advertir o aluno, sem o expor perante os demais ou ao ridículo, e levá-lo para a Direção da IMACULADA REDE DE EDUCAÇÃO, a fim de que se tomem as medidas disciplinares e legais apropriadas, bem como sejam avisados seus responsáveis legais imediatamente.

DISPOSIÇÕES FINAIS

6.1. O presente documento será complementado pelas regras de Segurança da Informação da IMACULADA REDE DE EDUCAÇÃO e está em consonância com a norma ABNT NBR ISO/IEC 27002:2013 – “Código de prática para controles de segurança da informação”, o Estatuto da Criança e do Adolescente, a Lei de Diretrizes e Bases da Educação Nacional e com a legislação vigente no Brasil.

6.2. A IMACULADA REDE DE EDUCAÇÃO é responsável pela divulgação deste Guia e de suas regras complementares aos colaboradores e docentes.

6.3. Quaisquer atitudes ou ações indevidas, antiéticas, ilícitas, imorais, não autorizadas ou contrárias ao recomendado por este Guia ou pelas demais regras da IMACULADA REDE DE EDUCAÇÃO, **inclusive a tentativa de burla**, serão consideradas violações por si só e estarão sujeitas às medidas previstas no Regimento Escolar e nas suas demais regras.

6.4. Dentre as medidas cabíveis aplicadas estão, mas não se limitando a advertência verbal ou escrita e suspensão de uso do RETIC institucional ou particular em proveito da Escola em suas dependências, podendo

resultar até em rescisão de contrato ou desligamento por justa causa, conforme a natureza e gravidade da conduta.

- 6.5.** A aplicação das medidas disciplinares e/ou administrativas não afasta eventual instauração de procedimentos judiciais e/ou administrativos internos, além da responsabilidade pelos prejuízos causados.
- 6.6.** Este Guia e as demais regras de Segurança da Informação da IMACULADA REDE DE EDUCAÇÃO encontram-se disponíveis no site <http://s2.alunoonline.net/meninojesus/professor> na guia “Materiais” ou em caso de indisponibilidade, podem ser solicitadas para a Direção.
- 6.7.** Em caso de dúvidas quanto a este Guia ou aos demais procedimentos de Segurança da Informação da IMACULADA REDE DE EDUCAÇÃO, o colaborador ou docente pode solicitar os esclarecimentos necessários por meio do e-mail esc.escmeninojesus@escmeninojesus.com.br.
- 6.8.** Em caso de incidente, infração ou a suspeita de qualquer dessas ocorrências, a Direção deverá ser comunicada imediatamente.
- 6.9.** Este Guia é um documento jurídico que trata da organização escolar, em complemento às demais regras pedagógicas e de gestão da Escola e deve ser interpretado no idioma português e sob a égide das leis brasileiras.

TERMOS E DEFINIÇÕES

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano à Escola.

Aplicativos de comunicação: Conjunto de código e instruções compiladas, executadas ou interpretadas por um recurso tecnológico, hospedadas em um dispositivo ou na nuvem, que é usada para troca rápida de mensagens, conteúdos e informações multimídia.

Ativo: É qualquer coisa que tenha valor para a Escola e precisa ser adequadamente protegido.

Ativo Intangível: Todo elemento que possui valor para a IMACULADA REDE DE EDUCAÇÃO e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à reputação, imagem, marca e conhecimento.

Autenticidade: Garantia de que a informação seja procedente e fidedigna, sendo a mesma, capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

Backup: Salvaguarda de sistemas ou arquivos, realizada por meio de reprodução e/ou espelhamento de uma base de arquivos, com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de *roll back*, ou constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada da IMACULADA REDE DE EDUCAÇÃO.

Confidencialidade: Garantia que as informações sejam acessadas somente por aqueles expressamente autorizados e sejam devidamente protegidas do conhecimento alheio.

Colaborador: Empregado, docente, estagiário, prestador de serviço, terceirizado, conveniado, credenciado, fornecedor, cliente, menor aprendiz, ou qualquer outro indivíduo ou organização que venham a ter relacionamento, direta ou indiretamente, com a IMACULADA REDE DE EDUCAÇÃO.

Disponibilidade: garantia de que as informações e os RETIC estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

Dispositivos Móveis: Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente transportados devido a sua portabilidade, como por exemplo, pen drive, celular, *smartphone*, computadores portáteis, *tablet*, equipamento reproduzidor de MP3, câmeras de fotografia ou filmagem, ou qualquer dispositivo que permita conexão à Internet (tais como dispositivos 3G e Wi-Fi), portabilidade ou armazenagem de dados.

Homologação: Processo de avaliação e aprovação técnica de RETIC e de aplicativo que antecede sua aquisição ou utilização.

Identidade Digital: É a identificação do colaborador/docente em ambientes lógicos, sendo composta por seu nome de usuário (*login*) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, *token* e biometria.

Incidente de Segurança da Informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação ao Guia ou às regras de Segurança da Informação, falha de controles, ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

Informação: A informação é o conjunto de dados que, processados ou não, podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Integridade: Garantia de que as informações estejam íntegras durante o seu ciclo de vida.

Internet: Rede mundial de computadores, na qual o usuário pode, a partir de um dispositivo, caso tenha acesso e autorização, obter informação de qualquer outro dispositivo que também esteja conectado à rede. O protocolo padrão utilizado na Internet é o TCP/IP.

Legalidade: garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor no Brasil.

Login: Identificação única dos usuários para acessarem sistemas computacionais ou RETIC.

Recursos Educacionais de Tecnologia da Informação e Comunicação: São todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação. Entre os tipos de recursos podemos destacar: microcomputador, computadores portáteis, *smartphones*, *tablets*, *pen drive*, mídias, discos externos, impressoras, scanner, entre outros. Sempre que mencionados de forma a não identificar seu possuidor ou proprietário, os RETIC compreenderão tanto os pertencentes à IMACULADA REDE DE EDUCAÇÃO quanto aos particulares em proveito institucional. Caso contrário, haverá declinação de posse ou propriedade no próprio texto.

Risco: Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

Violação: Qualquer atividade que desrespeite as diretrizes estabelecidas no Guia ou em quaisquer das demais regras que as complementem, inclusive a mera tentativa ou burla.



PATRICIA PECK PINHEIRO
Advogados Especialistas em Direito Digital