COLÉGIO PRESBITERIANO MACKENZIE

Cartilha de Proteção de Dados

Boas Práticas para o dia a dia escolar

CLÍNICA JURÍDICA HABILIDADOS

Sumário

— Apresentação 03

01 O que é a LGPD e por que ela importa 04

02 Conceitos 05

03 Coleta e uso de dados 10

04 Armazenamento e Descarte de Dados 12

05 Compartilhamento de dados pessoais 14

06 Segurança da Informação 17

07 Situações que exigem cuidado especial 19

08 Direitos dos Titulares 21

09 Incidentes de Segurança — o que fazer? 22

10 O Papel de Cada Colaborador 23

11 Perguntas Frequentes 24

12 Canais de contato 26

Apresentação

Esta cartilha foi criada para você, colaborador do Colégio Presbiteriano Mackenzie, que no dia a dia lida com informações pessoais de alunos, responsáveis e colegas de trabalho.

Queremos que você termine a leitura se sentindo mais confiante para usar dados pessoais em situações comuns do ambiente escolar.

Cuidar bem dos dados pessoais de alunos e famílias é parte da missão do Mackenzie e do compromisso com sua comunidade. E você é peça fundamental nesse processo.

PARA QUE SERVE ESTA CARTILHA?

- Explicar o que é a Lei Geral de Proteção de Dados (LGPD) e porque ela importa;
- Orientar como agir nas situações comuns do cotidiano escolar que envolvam dados pessoais;
- Indicar quando e como compartilhar informações pessoais de forma segura;
- Mostrar o que fazer em caso de dúvida ou problema.

CAPÍTULO UM

01 O que é a LGPD e por que ela importa

1.1 A lei em poucas palavras

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD) estabelece as regras para coletar, usar, guardar, compartilhar e até descartar informações pessoais no Brasil. Ela vale para empresas, escolas, hospitais e qualquer pessoa ou organização que trate dados de pessoas.

O objetivo central da lei é garantir que as informações de cada pessoa sejam usadas com respeito, transparência e segurança, protegendo direitos fundamentais como a privacidade, a liberdade e o livre desenvolvimento de cada pessoa.

1.2 Por que devemos nos importar?

Lidamos diariamente com informações de alunos, responsáveis e colaboradores. Um dado pessoal compartilhado de forma errada ou descartado inadequadamente pode:

- Expor informações privadas de crianças e adolescentes;
- Causar danos à imagem e à confiança que as famílias depositam na instituição;
- Gerar consequências legais e financeiras para o colégio.

Proteger dados vai além de ser uma obrigação legal. É também uma forma de cuidar das pessoas.

DOIS CONCEITOS QUE ANDAM JUNTOS

Privacidade

É a possibilidade que cada pessoa tem de decidir o que quer manter reservado sobre si mesma, o que compartilha, com quem e em qual situação.

Proteção de dados

São os cuidados práticos que tomamos para que esse direito seja respeitado.

02 Conceitos

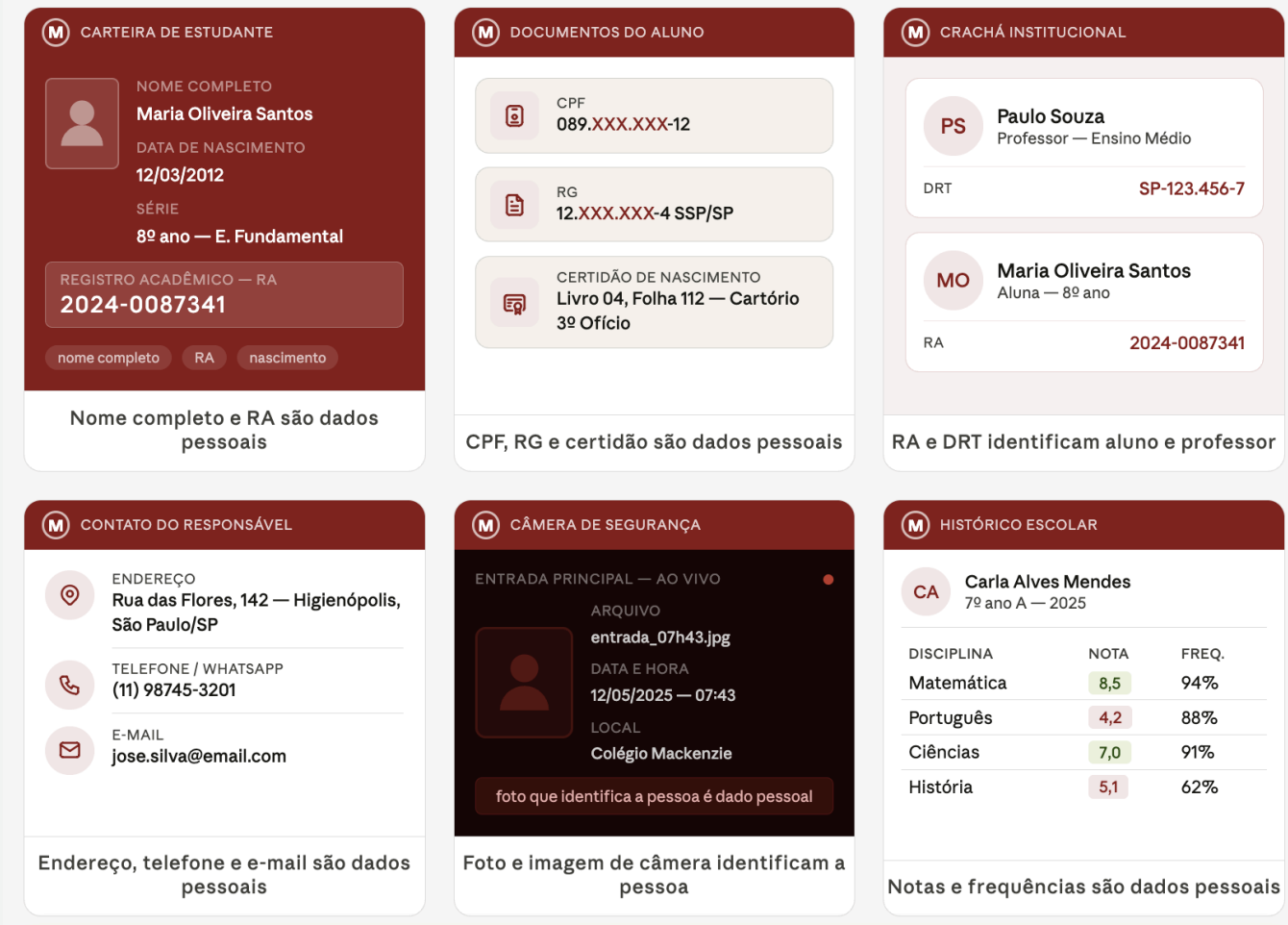
CAPÍTULO DOIS

2.1 O que são dados pessoais?

Dado pessoal é qualquer informação que identifica ou pode identificar uma pessoa.

Pode ser um documento oficial, uma foto, um número de telefone ou até um apelido pode ser um dado pessoal dependendo do contexto.

EXEMPLOS NO AMBIENTE ESCOLAR:

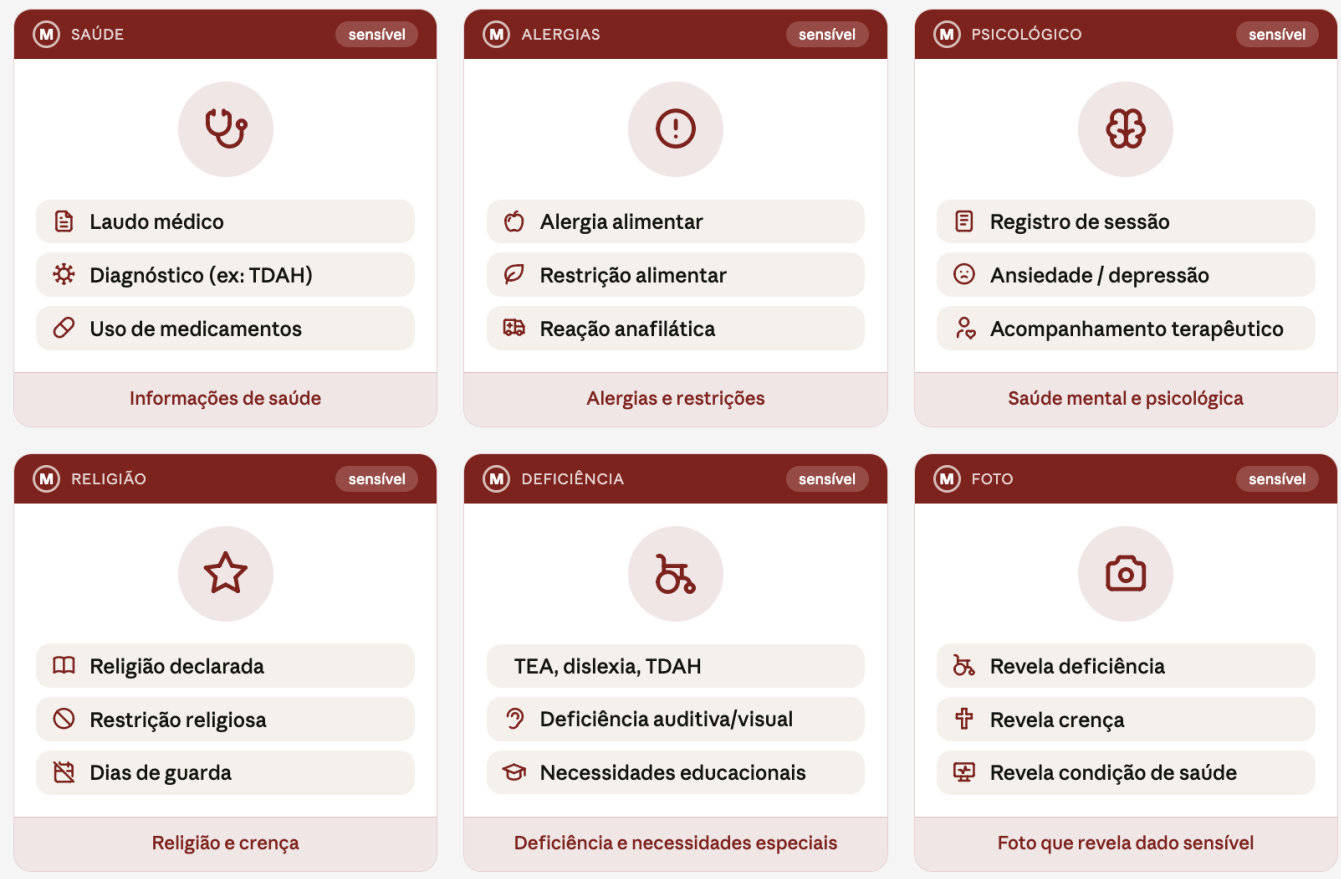


2.2 O que são dados pessoais sensíveis?

Alguns dados merecem atenção maior porque, se expostos, podem gerar discriminação ou causar danos mais sérios à pessoa, que chamamos de dados sensíveis. Como:

- origem racial ou étnica;
- religião, opinião política, filiação a sindicatos ou organizações religiosas e filosóficas;
- dados genéticos e biométricos;
- dados de saúde e vida sexual.

No ambiente escolar, esses dados aparecem frequentemente e exigem cuidado redobrado. Veja alguns exemplos:



2.3 Os princípios que orientam o uso de dados pessoais

A LGPD estabelece princípios que funcionam como um guia de conduta para qualquer pessoa que lide com informações pessoais:

Finalidade

Use o dado só para o motivo pelo qual ele foi coletado. Um dado de matrícula não pode ser usado para outra finalidade sem uma justificativa aceitável e que encontra respaldo na LGPD.

Adequação

O uso do dado precisa estar alinhado com a finalidade informada ao titular, respeitando o contexto em que esse dado foi coletado. Pergunte-se: esse uso está coerente com o que foi explicado à pessoa no momento da coleta? Ele faz sentido dentro dessa situação?

Necessidade

Colete e use apenas o mínimo necessário.

Livre acesso

O titular tem direito de saber quais dados o colégio tem sobre ele e como estão sendo usados.

Qualidade

Mantenha os dados corretos e atualizados. Informações desatualizadas podem causar erros graves.

Transparência

Seja claro sobre como e por que os dados estão sendo usados.

Segurança

Proteja os dados contra acessos não autorizados, perdas ou vazamentos.

Prevenção

Antecipe riscos antes que aconteçam. Não espere o erro para agir.

Não discriminação

Dados pessoais não podem ser usados para discriminar ou prejudicar alguém.

Responsabilização

Cada um é responsável pelo uso que faz dos dados. E precisa ser capaz de demonstrar que agiu corretamente.

2.4 Quais são as justificativas que permitem o uso de dados pessoais?

01 **Consentimento** — o titular (ou o responsável legal, no caso de crianças ou adolescentes) autoriza expressamente aquele uso específico do dado. Ex: para utilização de foto em campanhas publicitárias.

02 **Cumprimento de obrigação legal** — a lei exige o tratamento daquela informação. Por exemplo: enviar dados dos alunos a órgãos reguladores como o MEC, quando necessário.

03 **Estudos e pesquisas** — quando o dado é usado por instituições de ensino superior e de pesquisa, seguindo os critérios da Lei e das resoluções.

04 **Execução de contrato** — o uso do dado é necessário para cumprir o contrato de matrícula ou para prestar o serviço educacional contratado pela família.

05 **Exercício de direitos** — o dado é necessário para você se defender ou atuar em um processo judicial, administrativo ou arbitral. Ex: apresentação de dados do aluno em processos judiciais no qual o Mackenzie é parte.

06 **Proteção da vida** — há necessidade de proteger a vida ou a integridade física do aluno ou de terceiros. Por exemplo: uma emergência médica.

07 **Cuidado com a saúde** — profissionais de saúde, como a enfermaria, precisam de informações para cuidar do aluno.

08 **Interesse legítimo** — você tem um interesse legítimo no uso daquele dado, desde que isso não prejudique os direitos do titular. Por exemplo: uso de câmeras para a segurança das dependências escolares.

09 **Proteção de crédito** — quando o dado é necessário para análises ligadas a pagamentos e inadimplência.

Para dados sensíveis, vale a mesma lista acima, mas atenção, com duas diferenças:

Não servem como justificativa para dados sensíveis:

- Interesse legítimo
- Proteção de crédito
- Execução de contrato (só vale quando ligada ao exercício de um direito, não para qualquer uso contratual)

Aparece uma nova hipótese para dados sensíveis:

- **Prevenção a fraudes** — quando o dado sensível (como biometria) é usado para autenticação e segurança em sistemas eletrônicos.

Na prática, isso significa que sempre precisa existir uma dessas justificativas para cada uso de dados pessoais. Na dúvida sobre qual se aplica à sua situação, consulte a DPO.

OBSERVAÇÃO

Toda base legal precisa ser usada junto com os princípios do tópico 2.3 — especialmente finalidade, necessidade, segurança e adequação. Ou seja: mesmo com uma justificativa válida, você só pode usar o mínimo necessário, para aquele propósito específico, da forma que foi informada ao titular e de maneira zelosa.

CAPÍTULO TRÊS

03 Coleta e uso de dados

3.1 Como as informações chegam até você?

Os dados podem chegar por vários caminhos:

- pelo sistema interno,
- por e-mail,
- por documentos físicos entregues pelos responsáveis,
- por conversas com colegas,
- por aplicativos de mensagem.

Independentemente do meio, os dados devem trafegar pelos canais mais seguros disponíveis e nunca por canais pessoais ou não autorizados.

3.2 Quais dados você pode acessar?

O acesso às informações pessoais deve ser restrito à sua função.

No Mackenzie, há um controle de acesso rigoroso nos sistemas. Cada colaborador vê apenas o que é necessário para o exercício do seu trabalho.

ATENÇÃO

Se você se deparar com informações que não fazem parte da sua atividade, não as utilize e comunique ao seu superior imediato. Acessar dados que não dizem respeito à sua função pode configurar desvio de conduta.

3.3 Quando preciso de autorização para usar dados?

Nem sempre o uso de dados exige autorização expressa da pessoa a quem o dado pertence. Há situações em que o uso é permitido mesmo sem consentimento, como para cumprir obrigação legal ou para proteger a vida do aluno.

Mas atenção: mesmo quando não é exigida autorização, o uso deve sempre ter uma finalidade legítima e ser o mínimo necessário.

EXEMPLOS DE USO PERMITIDO SEM CONSENTIMENTO

- Enviar histórico escolar para órgãos educacionais (obrigação legal);
- Acionar o pronto-socorro com dados médicos do aluno em situação de emergência (proteção da vida);
- Informar dado de aluno ao Conselho Tutelar quando exigido (obrigação legal).

ATENÇÃO!

Avós, tios e outros parentes que não possuam a guarda legal do aluno não são considerados responsáveis legais. Eles não têm direito automático de receber informações sobre o estudante.

CAPÍTULO QUATRO

04 Armazenamento e Descarte de Dados

4.1 Onde os dados devem ficar guardados?

Todas as informações de alunos, responsáveis, colaboradores e prestadores de serviço devem ser armazenadas em sistemas digitais ou locais físicos controlados e aprovados pela Gerência de Tecnologia da instituição (GERTI).

O QUE FAZER

- Usar os sistemas internos homologados pelo Mackenzie;
- Guardar documentos físicos em armários trancados ou áreas restritas;
- Utilizar senhas fortes e bloquear a tela ao se afastar do computador;
- Manter apenas as informações necessárias pelo tempo necessário.

O QUE NÃO FAZER

- Salvar dados em dispositivos pessoais (celular, pendrive, notebook particular);
- Armazenar informações em e-mails pessoais ou ferramentas não autorizadas;
- Deixar documentos físicos com dados pessoais em locais de acesso livre;
- Acumular dados desnecessários sem prazo ou finalidade definida.

4.2 Por quanto tempo guardar as informações?

Os dados devem ser mantidos pelo tempo necessário para cumprir sua finalidade. Quando essa finalidade termina, os dados devem ser descartados de forma segura.

Atenção: antes de descartar, verifique se existe alguma obrigação legal que exija a manutenção daquela informação por um período determinado.

4.3 Como descartar dados corretamente?

DESCARTE SEGURO

Documentos físicos

- Utilize a fragmentadora de papel para destruir documentos com dados pessoais;
- Nunca descarte documentos inteiros em lixo comum;
- Não reutilize papéis que contenham dados pessoais de outras pessoas.

Documentos digitais

- Exclua de forma permanente os arquivos e e-mails que não têm mais utilidade;
- Verifique se a informação foi excluída de todos os locais onde estava armazenada (lixeira, cópias, backup);
- Não salve documentos com dados pessoais em dispositivos pessoais ou sem proteção de senha.

CAPÍTULO CINCO

05 Compartilhamento de dados pessoais

5.1 Antes de compartilhar, pergunte-se

CHECKLIST DO COMPARTILHAMENTO RESPONSÁVEL

Tem um motivo claro? Há uma razão legítima para esse compartilhamento?

É permitido? Existe uma base legal que autoriza?

É a pessoa certa? Quem vai receber realmente precisa dessa informação?

É só o necessário? Estou enviando o mínimo indispensável?

É um canal seguro? Estou usando uma ferramenta institucional? Se for por e-mail, protegi os dados com senha e enviei a senha por outro meio?

Tenho como comprovar? Existe um registro que respalde esse compartilhamento?

Se alguma resposta for não ou não tenho certeza, não compartilhe e consulte a DPO.

5.2 Com quem posso compartilhar?

O compartilhamento depende da situação. Veja as mais comuns:

Com a equipe interna

O compartilhamento de informações de alunos com colegas da equipe pedagógica, coordenação, orientação e direção será necessário sempre que houver necessidade relacionada ao atendimento do aluno e gerenciamento do contrato de prestação de serviços educacionais. Porém, compartilhe apenas com quem precisa e apenas as informações necessárias para aquela situação.

Com médicos, psicólogos e outros profissionais de saúde

É permitido, quando autorizado expressamente pelos pais ou responsáveis, ou quando houver necessidade para proteção da vida ou para cuidar da saúde do aluno. Nesses casos, compartilhe apenas o que for estritamente relevante e com acesso restrito aos profissionais envolvidos no atendimento.

Com órgãos públicos e poder judiciário

Pode ser necessário em casos específicos, como solicitações do Conselho Tutelar, Ministério Público, Autoridade Policial ou determinações judiciais. Nesses casos, siga os procedimentos institucionais e envolva sempre a DPO.

Com responsáveis ou familiares do mesmo aluno

Somente com quem possui guarda legal. Avós, tios e outros parentes sem guarda formal não têm direito automático a receber essas informações.

Com responsáveis de outros alunos

Regra geral: não. Apenas em situações específicas e com amparo legal. Na dúvida, consulte a DPO antes.

5.3 Posso enviar dados por e-mail com outras pessoas em cópia?

Depende. O compartilhamento nestes casos é permitido desde que todas as pessoas copiadas realmente precisem daquela informação e tenham uma finalidade legítima para recebê-la.

Antes de adicionar alguém em cópia, pergunte-se: essa pessoa precisa mesmo estar aqui?

5.4 Como enviar arquivos com dados pessoais por e-mail?

O QUE FAZER

- Usar sempre o e-mail institucional;
- Enviar planilhas e documentos protegidos por senha;
- Enviar a senha por outro canal (ex: telefone ou mensagem separada);
- Confirmar que os destinatários são as pessoas certas antes de enviar.

O QUE NÃO FAZER

- Usar e-mail pessoal para enviar dados de alunos ou responsáveis;
- Enviar documentos sem proteção de senha;
- Copiar pessoas que não precisam daquela informação;
- Usar WhatsApp ou aplicativos de mensagem pessoal para trafegar dados.

Não compartilhe dados pessoais de alunos fora das ferramentas institucionais do Mackenzie. Isso inclui WhatsApp pessoal, e-mail particular e qualquer plataforma não homologada pela GERTI.

CAPÍTULO SEIS

06 Segurança da Informação

6.1 Suas credenciais de acesso são sua responsabilidade

O login e a senha que você usa para acessar os sistemas do colégio são pessoais e intransferíveis. Compartilhar suas credenciais com outro colaborador, mesmo que por um momento, é uma violação das normas de segurança do Mackenzie.

Lembre-se: os sistemas registram quem acessou cada informação. Se alguém usar seu login para acessar dados de forma indevida, você poderá ser responsabilizado.

COMO PROTEGER SUAS CREDENCIAIS

- ☐ Crie senhas fortes (misture letras maiúsculas, minúsculas, números e símbolos)
- ☐ Não anote senhas em papéis ou arquivos abertos
- ☐ Não compartilhe sua senha com ninguém, nem com colegas de confiança
- ☐ Troque a senha periodicamente ou quando suspeitar de uso indevido
- ☐ Bloqueie a tela do computador sempre que se afastar, mesmo que por poucos minutos



CREDENCIAIS

Seu login e sua senha são pessoais e intransferíveis.

6.2 Cuidados com e-mails suspeitos

Golpes por e-mail (phishing) são uma das formas mais comuns de acesso indevido a sistemas e dados. Aprenda a reconhecê-los:

SINAIS DE ALERTA EM E-MAILS

- E-mails pedindo que você clique em links e insira seus dados
- Remetente desconhecido ou com endereço estranho (ex: mackenzie@gmail.com)
- Mensagens com urgência excessiva: 'Sua conta será bloqueada em 24 horas'
- Erros de português ou formatação estranha
- Pedido de senha ou dados pessoais por e-mail

Em caso de dúvida, não clique em nada e comunique imediatamente à GERTI.

6.3 Uso seguro de dispositivos

O QUE FAZER

- Acessar dados de alunos apenas em dispositivos institucionais;
- Manter o antivírus e o sistema operacional atualizados;
- Usar apenas sistemas e aplicativos homologados pela GERTI;
- Relatar ao e-mail si@mackenzie.br qualquer comportamento estranho no seu computador.

O QUE EVITAR

- Salvar documentos com dados pessoais em dispositivos particulares;
- Usar redes de Wi-Fi públicas para acessar sistemas do Mackenzie;
- Instalar programas não autorizados nos computadores do colégio.

LEMBRETE

O Curso de LGPD da Academia Corporativa do Mackenzie é obrigatório para todos os colaboradores. Se você ainda não realizou, não perca tempo!

CAPÍTULO SETE

07 Situações que exigem cuidado especial

7.1 Dados de saúde

Como vimos no tópico 2.2, dados de saúde são considerados sensíveis e exigem proteção redobrada. No dia a dia do colégio, isso inclui laudos, diagnósticos, alergias, uso de medicamentos e, algumas vezes, acompanhamento psicológico.

O QUE FAZER

- Compartilhar informações de saúde apenas com quem diretamente precisar para cuidar do aluno;
- Usar canais seguros e institucionais para transmitir esse tipo de dado;
- Solicitar laudo médico atualizado a cada renovação de matrícula;
- Armazenar laudos e fichas médicas em locais restritos e seguros.

O QUE É PROIBIDO

- Comentar sobre condições de saúde de alunos em espaços informais;
- Compartilhar laudos em grupos de WhatsApp ou e-mails amplos;
- Guardar fichas médicas em locais de acesso livre;
- Repassar informações de saúde para outros responsáveis sem necessidade ou permissão legal.

7.2 Questões familiares

Situações como separação de responsáveis, guarda judicial, medidas protetivas e conflitos familiares são informações delicadas. Quem tem acesso a elas precisa tratá-las com discrição.

BOAS PRÁTICAS

- Compartilhe apenas com a equipe diretamente envolvida no caso;
- Evite comentários ou conversas informais sobre a situação familiar do aluno;
- Nunca compartilhe informações familiares com outros responsáveis sem amparo legal.

7.3 Crianças e adolescentes têm proteção especial

Lidamos com informações pessoais que envolvem crianças e adolescentes. Isso significa uma responsabilidade a mais: qualquer decisão sobre esses dados deve ser tomada pensando sempre no melhor interesse de crianças e adolescentes, não na conveniência do processo, nem na facilidade do momento.

Na prática, isso quer dizer:

- Não publique imagens de alunos em grupos, redes sociais ou qualquer canal sem autorização;
- Só utilize ferramentas homologadas pela instituição. Um aplicativo não autorizado que coleta dados de alunos é uma violação, mesmo que seja "só para facilitar a comunicação";
- Compartilhamento com responsáveis — apenas o responsável legal pode receber informações sobre o aluno;
- Laudos e informações sensíveis — não discuta condições de saúde, diagnósticos ou situações familiares de alunos em conversas informais, grupos de WhatsApp ou e-mails amplos;
- Se não há clareza sobre quem pode receber determinada informação, não compartilhe. Consulte a DPO antes de agir.



As decisões devem acontecer sempre pensando no melhor interesse de crianças e adolescentes.

CAPÍTULO OITO

08 Direitos dos Titulares

8.1 Quais são os direitos de alunos e responsáveis?

A LGPD garante uma série de direitos a qualquer pessoa cujos dados sejam tratados pela instituição, isso inclui alunos, professores e colaboradores.

OS TITULARES TÊM DIREITO DE:

- Saber quais dados o colégio possui sobre eles e como são utilizados
- Solicitar correção de informações incorretas ou desatualizadas
- Pedir esclarecimentos sobre o uso dos dados
- Solicitar acesso às próprias informações

8.2 O que fazer quando um aluno ou responsável fizer uma solicitação?

Se um aluno ou responsável entrar em contato pedindo acesso aos seus dados, solicitando correção de informações ou fazendo qualquer outro pedido relacionado aos seus direitos, você deve encaminhar a demanda para a DPO imediatamente.

O colégio já tem procedimentos internos definidos para isso. O importante é não tomar decisões sozinho.

CONTATO DA DPO DO MACKENZIE

dpo.cmpd@mackenzie.br

8.3 Limites ao pedido de exclusão

Nem todo pedido de exclusão de dados pode ser atendido imediatamente. Em alguns casos, a lei obriga o colégio a manter determinadas informações por um período específico. A DPO é a pessoa indicada para avaliar esses casos.

CAPÍTULO NOVE

09 Incidentes de Segurança

9.1 O que é um incidente de segurança?

Um incidente de segurança com dados pessoais é qualquer situação que resulte em acesso não autorizado, perda, alteração, compartilhamento indevido ou destruição de dados pessoais.

EXEMPLOS

- E-mail enviado para o destinatário errado contendo dados de alunos
- Computador roubado ou perdido com informações não criptografadas
- Acesso indevido ao sistema por pessoa não autorizada
- Compartilhamento de dados em grupo de WhatsApp por engano

9.2 O que fazer se você perceber um incidente?

AJA RAPIDAMENTE

- Não tente resolver sozinho ou encobrir o ocorrido
- Comunique imediatamente ao seu superior hierárquico
- Comunique a GERTI (TI) e a DPO: dpo.cmpd@mackenzie.br
- Registre o máximo de informações sobre o que aconteceu (quando, o quê, como)
- Preserve as evidências e não altere nada até ser orientado.



Quanto mais rápido o incidente for reportado, menor pode ser o impacto.

CAPÍTULO DEZ

10 O Papel de Cada Colaborador

A proteção de dados não é responsabilidade exclusiva da TI ou da DPO. Cada colaborador, independentemente do cargo, têm um papel fundamental nesse processo.

Pequenas atitudes do dia a dia — como não compartilhar a senha, não enviar dados por WhatsApp pessoal e consultar a DPO em caso de dúvida — fazem uma diferença enorme.

A cultura de proteção de dados

Proteção de dados não deve ser vista como uma burocracia ou um obstáculo. É uma expressão de respeito pelas pessoas que confiam ao Mackenzie as informações mais importantes de suas vidas.

Sanções e consequências

O descumprimento da LGPD pode gerar consequências tanto para a instituição quanto para o colaborador individualmente. Entre as sanções previstas para as organizações estão advertências, multas e publicização da infração.

Do ponto de vista interno, o uso indevido de dados pode configurar desvio de conduta e resultar em medidas disciplinares.



Pequenas atitudes do dia a dia fazem uma grande diferença.

CAPÍTULO ONZE

11 Perguntas Frequentes

Posso usar o WhatsApp para enviar dados de alunos?

Não. Dados pessoais de alunos e responsáveis não devem ser trafegados por aplicativos de mensagem pessoal, como WhatsApp. Utilize os canais institucionais.

Posso tirar fotos de documentos de alunos no meu celular?

Não é recomendado. Salvar dados de alunos em dispositivos pessoais representa um risco de segurança. Se houver necessidade de registro, utilize os sistemas homologados pela GERTI.

Um responsável pediu informações sobre outro aluno. O que faço?

Não compartilhe. Regra geral, as informações de um aluno não podem ser compartilhadas com responsáveis de outros alunos. Encaminhe a demanda para a DPO.

Recebi um laudo médico de um aluno por e-mail. O que devo fazer?

Armazene no sistema interno autorizado e garanta que apenas as pessoas que precisam dessa informação tenham acesso. Não encaminhe para grupos, não salve em dispositivos pessoais.

Posso comentar com colegas sobre situações familiares delicadas de um aluno?

Somente quando houver necessidade direta para o atendimento do aluno e com os colegas diretamente envolvidos. Evite comentários informais sobre situações privadas.

Um colega pediu minha senha para acessar o sistema. O que faço?

Não compartilhe. Suas credenciais são pessoais e intransferíveis. Se o colega precisa de acesso, ele deve solicitar às áreas responsáveis pela concessão de permissões.

Tenho dúvida se posso ou não compartilhar uma informação. O que faço?

Na dúvida, não compartilhe. Consulte a DPO (dpo.cmpd@mackenzie.br) antes de agir.

Recebi dados de alunos que não fazem parte da minha função. O que faço?

Não utilize esses dados. Informe ao seu superior hierárquico.

Mandei um e-mail com dados de alunos para o destinatário errado. O que faço?

Comunique imediatamente ao seu superior, à GERTI e à DPO. Não tente resolver por conta própria. Quanto mais rápido o incidente for reportado, menor o impacto.

O Curso de LGPD da Academia Corporativa é obrigatório?

Sim. Todos os colaboradores do Mackenzie devem realizá-lo. Se você ainda não fez, procure sua liderança.



NA DÚVIDA

Não compartilhe. Consulte a DPO antes de agir.

12 CAPÍTULO DOZE
Canais de contato

Fale com a DPO

E-mail: dpo.cmpd@mackenzie.br

USE ESTE CANAL PARA

- Tirar dúvidas sobre como agir em situações específicas;
- Reportar incidentes de segurança com dados pessoais;
- Encaminhar solicitações de titulares (alunos ou responsáveis);
- Obter orientação sobre o compartilhamento de dados em casos específicos.

Clínica Jurídica Habilidados

Este material foi desenvolvido pela Clínica Jurídica Habilidados, projeto de extensão da Faculdade de Direito da Universidade Presbiteriana Mackenzie, em parceria com a DPO do Instituto Presbiteriano Mackenzie e com o Comitê Mackenzie de Proteção de Dados. A Clínica atua voluntariamente para democratizar o acesso à proteção de dados pessoais em comunidades e instituições vinculadas à universidade.

Coordenadora da Clínica: Maria Rita Neiva

Orientadora da Clínica: Natália Ribeiro

Autores: Ana Júlia de Aquino Codelo; Ariadne Oliveira Felix; Davi Vilas Boas Senteio; Lucas Vilela Picca; Maria Eduarda Ferraz; Matheus Costa de Lima.


Mackenzie