POLÍTICA INSTITUCIONAL DE PROTEÇÃO DE DADOS PESSOAIS

31 DE JANEIRO DE 2025

INSTITUTO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA
Rua Madre Beatriz Frambach, nº. 84, bairro Dom Cabral
Belo Horizonte – MG

Sumário

APRESENTAÇÃO 4
Capítulo 1. Introdução 5

1. Conceitos e Definições 5
2. Abreviações Importantes 6
3. Dos Objetivos e dos Princípios Norteadores desta Política Institucional de Proteção de Dados Pessoais 6
4. Da Abrangência desta Política Institucional de Proteção de Dados Pessoais 8

Capítulo 2. Dos Envolvidos com a Proteção de Dados Pessoais no IISNS 9

5. Do Comitê de Segurança da Informação 9
6. Do Encarregado de Dados Pessoais (Data Protection Officer – DPO) 9
7. Dos Colaboradores do IISNS 11

Capítulo 3. Do Tratamento de Dados Pessoais 12

Seção 1. Disposições Comuns à Qualquer Tratamento de Dados Pessoais 12

8. Sobre o Tratamento de Dados Pessoais 12
9. Sobre o Tratamento de Dados Pessoais da Criança e do Adolescente 14
10. Da Classificação dos Dados Pessoais Tratados 14
11. Dos Níveis de Acesso e de Sigilo 15
12. Da Eliminação dos Dados Pessoais 15

Seção 2. Dados Pessoais Tratados em Meios Físicos 15

13. Conceito 15
14. Dos Arquivos Físicos 16

Seção 3. Dos Dados Pessoais Tratados em Meios Digitais 16

15. Conceito 16
16. Do Compartilhamento de Dados Pessoais Tratados em Meios Digitais 16
17. Da Política de Cookies 17

Seção 4. Dos Sistemas utilizados pelo IISNS 17

18. Da Criação da Conta Corporativa 17
19. Do Cancelamento da Conta Corporativa 18

Seção 5. Do Sistema de Monitoramento por Câmeras 18

20. Conceitos e Definições 18
21. Da Guarda de dados/informações/arquivos no Sistema 18
22. Da Solicitação de Interessados 18

Seção 6. Dos Titulares de Dados Pessoais..... 19

23. Do Exercício dos Direitos dos Titulares..... 19

Capítulo 4. Do Plano de Resposta a Incidentes 20

24. Do Comitê de Crise 20
25. Dos Incidentes Envolvendo Dados Pessoais Tratados pelo IISNS e/ou por um dos seus Operadores..... 20
26. Da Análise e Da Avaliação dos Incidentes pelo Comitê de Crise 21
27. Dos Procedimentos a Serem Adotados pelo Comitê de Crise e demais Agentes Internos 21

Capítulo 5. Disposições Finais e Transitórias 23

28. Da Revisão desta Política Institucional de Proteção de Dados Pessoais 23

ANEXO 01 – Tabela de Temporalidade de Dados 24
ANEXO 02 – Tratamentos de Dados Específicos 28
ANEXO 03 – Termo para Alunos 31

1. Do Consentimento/Autorização de Tratamento 31
2. Das Disposições Finais 32

ANEXO 04 – Termo para Empregados 33

1. Do Consentimento/Autorização de Tratamento 33
2. Das Disposições Finais 34

ANEXO 05 – Termo para Casa de Formação 35

1. Do Consentimento/Autorização de Tratamento 35
2. Das Disposições Finais 36

ANEXO 06 – Revogação do Consentimento 37
ANEXO 07 – Termo de Acesso à Pasta Compartilhada..... 38

1. Do Acesso à Pasta Compartilhada..... 38
2. Das Obrigações e das Responsabilidades do(a) Destinatário(a) 38
3. Da Política de Privacidade 39
4. Das Disposições Finais 39

ANEXO 08 – Termo de Compromisso para Acesso ao Sistema de Câmeras 40

1. Do acesso do(a) EMPREGADO(A) ao Sistema de Monitoramento por Câmeras 40
2. Das Obrigações do(a) EMPREGADO(A) 40
3. Da Política de Privacidade 41
4. Das Disposições Finais 41

ANEXO 09 – Termo de Compromisso para Uso de Conta Corporativa 42

1. Da Conta Corporativa e dos Perfis de Acesso criados para Uso do(a) EMPREGADO(A) 42
2. Das Obrigações do(a) EMPREGADO(A) 42
3. Da Política de Privacidade 43
4. Das Disposições Finais 43

ANEXO 10 – Relatório de Ocorrências relacionadas ao Tratamento de Dados Pessoais 44

APRESENTAÇÃO

Para que possa desenvolver a sua vocação e cumprir os seus objetivos, o IISNS se vale do *tratamento de dados pessoais* de diversos *titulares*. Este *ativo*, tão essencial para a Instituição, naturalmente precisa ser protegido, mais especificamente no que tange aos pilares da segurança da informação, quais sejam: a confidencialidade, a integridade e a disponibilidade dos *dados* que o compõem, especialmente os *dados pessoais*.

É este o cenário em que a *Política Institucional de Proteção de Dados Pessoais* do IISNS foi elaborada, produto de ampla análise, mapeamento e inventário de toda a informação (*latu sensu*) que possa ter transitado na Instituição em qualquer nível/permissão de acesso, independentemente de onde ela esteja: na forma física (documentos físicos/impressos); residente na memória de máquinas e dispositivos; armazenada em disco ou em trânsito.

Tudo isso com vista à prioridade do IISNS sobre a privacidade e a segurança dos *dados pessoais* e dos *dados pessoais sensíveis* de cada *titular*, além do seu comprometimento com a transparência sobre o respectivo tratamento destes *dados*.

Capítulo 1. Introdução

1. Conceitos e Definições

1.1. Para fins de cumprimento da Lei Geral de Proteção de Dados (LGPD – Lei nº. 13.709/2018) e para os fins da *Política Institucional de Proteção de Dados Pessoais* do IISNS, considera-se:

1.1.1. **Dado Pessoal:** toda informação relacionada a pessoa natural identificada ou identificável.

1.1.2. **Dado Pessoal Sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

1.1.3. **Dado Anonimizado:** dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

1.1.4. **Titular de Dados Pessoais:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

1.1.5. **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

1.1.6. **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

1.1.7. **Encarregado de Dados Pessoais:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a *Autoridade Nacional de Proteção de Dados* (ANPD).

1.1.8. **Tratamento:** toda *operação* realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

1.1.9. **Operação:** atividade ou tarefa que envolve o *tratamento* de dados pessoais em qualquer nível.

1.1.10. **Agentes de Tratamento:** o *controlador* e o *operador*.

1.1.11. **Agente Interno:** colaborador(a) do IISNS que, em qualquer nível de permissão e/ou acesso, realiza tratamento de dados pessoais controlados ou operados por ele (IISNS).

1.1.12. **Agente Externo:** pessoa natural ou jurídica:

1.1.12.1. Que presta e/ou oferece serviços à IISNS;

1.1.12.2. Que realiza *tratamento* de *dados pessoais* controlados ou operados pelo IISNS em qualquer nível de permissão, acesso e/ou compartilhamento; **e**

1.1.12.3. Cujos *dados pessoais* tratados tenham correlação com o serviço prestado à IISNS.

1.1.13. **Setor:** subdivisão de uma *Unidade* do IISNS, identificado pelo conjunto de atividades exercidas pelos *agentes internos* nele alocados.

1.1.14. **Segurança da Informação:** preservação da confidencialidade, da integridade e da disponibilidade dos *dados pessoais* tratados pela Instituição.

1.1.15. **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o *tratamento* de seus *dados pessoais* para uma *finalidade* determinada.

1.1.16. **Incidente de segurança:** *"violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento"* (art. 4º da *General Data Protection Regulation – GDPR*, lei europeia de proteção de dados pessoais na qual se inspirou a LGPD).

1.1.17. **Incidente de Segurança envolvendo Dados Pessoais:** qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do *titular* dos *dados pessoais*[1].

2. Abreviações Importantes

2.1. São abreviações que poderão ser utilizadas nesta *Política Institucional de Proteção de Dados Pessoais*:

2.1.1. **LGPD:** Lei Geral de Proteção de Dados.

2.1.2. **ANPD:** Autoridade Nacional de Proteção de Dados.

2.1.3. **PPI:** Política de Privacidade Institucional.

2.1.4. **PIPDP:** Política Institucional de Proteção de Dados Pessoais.

2.1.5. **CSI:** Comitê de Segurança da Informação.

2.1.6. **DPO:** *Data Protection Officer* / Encarregado de Dados Pessoais.

2.1.7. **DPIA/RIPDP:** *Data Protection Impact Assessment* / Relatório de Impacto à Proteção de Dados Pessoais.

3. Dos Objetivos e dos Princípios Norteadores desta Política Institucional de Proteção de Dados Pessoais

3.1. A *Política Institucional de Proteção de Dados Pessoais* (*PIPDP*) do IISNS tem como objetivos:

3.1.1. Salvaguardar a confidencialidade, a integridade e a disponibilidade dos *dados pessoais* tratados pela Instituição;

---

[1] Texto extraído de https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Último acesso em 19/06/2024.

3.1.2. Definir as medidas e os protocolos que devem ser adotados pelos colaboradores quando do *tratamento de dados pessoais*;

3.1.3. Zelar pela proteção dos dados pessoais tratados e pelo resguardo aos direitos dos titulares, em seus diversos aspectos, tudo à luz da Lei nº. 13.709/2018 (LGPD);

3.1.4. Estabelecer os métodos de *tratamento de dados pessoais* de forma a garantir que os usuários obtenham acesso à informação e aos ativos correspondentes, sempre que necessário e de acordo com a permissão atribuída a cada um;

3.1.5. Preservar a informação e a normalidade das atividades nos diferentes *Setores* em atividade;

3.1.6. Estabelecer procedimentos e recomendações que visam prevenir e responder a incidentes de segurança;

3.1.7. Preservar a reputação do IISNS, no que tange ao *tratamento de dados pessoais* sob sua responsabilidade.

3.2. Além dos objetivos já destacados, a *PIPDP* do IISNS foi construída de forma a observar a boa-fé, quando do tratamento de *dados pessoais*, bem como os princípios estampados no art. 6º da Lei nº. 13.709/2018 (LGPD), a saber:

3.2.1. **finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

3.2.2. **adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

3.2.3. **necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

3.2.4. **livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

3.2.5. **qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

3.2.6. **transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

3.2.7. **segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

3.2.8. **prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

3.2.9. **não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

3.2.10. **responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de

comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

4. Da Abrangência desta Política Institucional de Proteção de Dados Pessoais

4.1. A *Política Institucional de Proteção de Dados Pessoais* do IISNS abrange todos os colaboradores (*agentes internos*) da Instituição, em todos os níveis de acesso aos dados pessoais tratados.

Capítulo 2. Dos Envolvidos com a Proteção de Dados Pessoais no IISNS

5. Do Comitê de Segurança da Informação

5.1. O *Comitê de Segurança da Informação* foi instituído com a finalidade de adequar o IISNS às disposições da Lei nº. 13.709/2018 (LGPD), desde os trabalhos de análise e mapeamento do fluxo de dados pessoais, até a criação de procedimentos/protocolos com vistas às melhores práticas de *tratamento*.

5.2. É composto por:

5.2.1. Membros atuantes em cada uma das seguintes *Unidades* do IISNS:

5.2.1.1. Matriz (Escritório Central) – Belo Horizonte-MG;
5.2.1.2. Colégio Nossa Senhora das Graças – Patos de Minas-MG;
5.2.1.3. Colégio Padre Júlio Maria – Boa Esperança-MG;
5.2.1.4. Colégio Santa Terezinha – Manhumirim-MG;
5.2.1.5. Colégio São José – Niterói-RJ.

5.2.2. *Encarregado de Dados Pessoais* (DPO);
5.2.3. Consultoria Jurídica da Instituição.

5.3. São atribuições do *Comitê de Segurança da Informação*:

5.3.1. Auxiliar o *Encarregado de Dados Pessoais* (DPO), quando do exercício de suas atribuições, em especial:

5.3.1.1. No monitoramento do ambiente de coleta e armazenamento de dados/informações, especialmente no que tange à proteção dos dados mapeados;
5.3.1.2. No monitoramento do respeito ao ciclo de vida de cada dado mapeado;
5.3.1.3. Na disseminação da cultura de *compliance*, através da realização de apresentações e comunicados;
5.3.1.4. Na elaboração de regulamentações/padrões de segurança da informação;
5.3.1.5. Na elaboração de proteção dos dados em camadas;
5.3.1.6. Na elaboração do Plano de Resposta a Incidentes e eventual *Plano de Ação para Situações de Emergência*.

5.3.2. Em caso de eventuais *incidentes de segurança* envolvendo *dados pessoais* tratados pelo IISNS e/ou por um dos seus *operadores*, atuar, excepcionalmente, como *Comitê de Crise*, para fins de análise, avaliação, acompanhamento e solução de tais *incidentes*.

6. Do Encarregado de Dados Pessoais (Data Protection Officer – DPO)

6.1. O IISNS nomeará *Encarregado de Dados Pessoais* (*Data Protection Officer – DPO*), cujas atribuições incluem, entre outras:

6.1.1. Receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.

6.1.2. Receber comunicações da *Autoridade Nacional de Proteção de Dados* (ANPD) e adotar providências.

6.1.3. Monitorar o ambiente de coleta e armazenamento de dados/informações, especialmente no que tange à proteção dos dados mapeados.

6.1.4. Monitorar o respeito ao ciclo de vida de cada dado mapeado, em especial no que tange aos prazos mínimos de guarda destes, com o fim de atender à legislação pertinente.

6.1.5. Apoiar a revisão/atualização dos processos, a definição e a avaliação dos controles internos, seguindo as melhores práticas e a *Política Institucional de Proteção de Dados Pessoais* da Instituição.

6.1.6. Propor soluções adequadas para o gerenciamento do tratamento de dados por terceiros (*agentes externos*).

6.1.7. Coordenar a elaboração do relatório de impacto à proteção de dados pessoais (*DPIA – Data Protection Impact Assessment)*, contendo a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

6.1.8. Disseminar a cultura de *compliance*, através da realização de apresentações e comunicados.

6.1.9. Gerenciar o treinamento de colaboradores quanto à *Política de Proteção de Dados* da Instituição.

6.1.10. Atuar em parceria com os diversos *Setores* no tratamento das questões de *compliance* dos processos implantados.

6.1.11. Monitorar os riscos apontados no *mapeamento de dados*, assessorando os diversos *Setores* na melhoria dos processos e nas necessárias ações para a mitigação e para a eliminação daqueles (riscos).

6.1.12. Acompanhar a atualização do *mapeamento de dados* (inclusive arquivos físicos), sugerindo adequações e/ou complementações eventualmente necessárias.

6.1.13. Se inteirar sobre a disponibilização de dados à terceiros (*agentes externos*).

6.1.14. Se inteirar sobre a existência de autorização expressa dos titulares para o tratamento dos dados.

6.1.15. Se inteirar do ciclo de vida de cada *dado pessoal*, assessorando os diversos *Setores* no cumprimento do daquele (*ciclo de vida*).

6.1.16. Atuar ativamente, e em conjunto com o *Comitê de Segurança da Informação*, na elaboração de regulamentações/padrões de segurança da informação.

6.1.17. Atuar ativamente, e em conjunto com o *Comitê de Segurança da Informação*, na elaboração do *Plano de Ação para Situações de Emergência*.

6.2. A nomeação do *Encarregado de Dados Pessoais (*DPO*)* será registrada, também, na *Política de Privacidade Institucional* do IISNS, junto ao(s) canal(ais) de comunicação disponibilizado(s) para fins de lhe serem direcionadas reclamações, comunicações e solicitações de esclarecimentos.

7. Dos Colaboradores do IISNS

7.1. Os colaboradores (*agentes internos*) do IISNS deverão aplicar, de maneira mandatória, as disposições desta *Política Institucional de Proteção de Dados Pessoais*, bem como as regulamentações, orientações e direcionamentos vindos do *Comitê de Segurança da Informação*.

Capítulo 3. Do Tratamento de Dados Pessoais

Seção 1.Disposições Comuns à Qualquer Tratamento de Dados Pessoais

8. Sobre o Tratamento de Dados Pessoais

8.1. O *tratamento de dados pessoais* pelo IISNS estará intimamente ligado à respectiva *finalidade*, visando, assim, o desenvolvimento da atividade a que está atrelado.
8.2. O IISNS é ***controlador*** dos *dados pessoais* por ele coletados, salvo se a coleta ocorrer a pedido de algum *agente externo*, hipótese em que a figura e as responsabilidades de controlador recairão sobre este (*agente externo*).
8.3. Os *dados pessoais* tratados pelo IISNS são:

8.3.1. protegidos pelos procedimentos estabelecidos nesta *PIPDP*, com trilhas de auditoria para registrar autorizações, utilização, impactos e violações;
8.3.2. mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificado ou eliminado o *dado pessoal* mediante informação ou constatação de impropriedade ou em face de solicitação de remoção, nos limites das normas pertinentes, devendo a neutralização ou descarte do *dado pessoal* observar as condições e períodos da tabela de prazos de retenção de dados;
8.3.3. compartilhados somente para o estrito exercício das atividades relacionadas à sua atividade econômica e vocacional, ou para atendimento de políticas públicas aplicáveis;
8.3.4. revistos em periodicidade mínima **anual**, sendo eliminados aqueles que já não forem necessários, por terem cumprido sua finalidade ou por ter se encerrado o seu prazo de retenção.

8.4. Cada operação de tratamento de dados pessoais, estará ligada a um ou mais verbo, que expressará(ão) *"o que está sendo feito com os dados pessoais"*.
8.5. As medidas de proteção são intimamente ligadas ao *tratamento* (*verbo*) descrito, somado ao rol de dados pessoais tratados e aos seus respectivos titulares.
8.6. São *verbos* que orientarão as *operações* de *tratamento de dados pessoais* do IISNS:

8.6.1. **Acesso:** ato de obter e/ou visualizar dados.

Exemplo: acesso concedido à Contabilidade sobre os dados coletados e/ou produzidos pelo Setor Financeiro.

8.6.2. **Coleta:** ato de obter/recolher novos dados.

Exemplo: coleta de dados pessoais de responsáveis financeiros para o preenchimento do Contrato de Prestação de Serviços de Educação Escolar.

8.6.3. **Extração:** ato de copiar ou de retirar dados de um repositório.

Exemplo: digitalizar fichas cadastrais.

8.6.4. **Produção:** ato de criar ou de gerar dados.

Exemplo01: dados relacionados à saúde do(a) empregado(a) gerados pela Medicina do Trabalho.
Exemplo02: elaboração do histórico escolar dos alunos.

8.6.5. **Recepção:** ato de receber dados por meio de compartilhamento, difusão, distribuição, transferência ou transmissão.

Exemplo: o Departamento Pessoal recebe Atestados de Saúde Ocupacionais (ASOs) da Medicina do Trabalho.

8.6.6. **Armazenamento:** ato de conservar ou manter dados em um repositório *"ativo"* (utilizado no dia a dia).

Exemplo: armazenamento de dados em uma rede interna de computadores da Instituição.

8.6.7. **Arquivamento:** ato de conservar ou manter dados em um repositório *"inativo"*, logo, não são utilizados no dia a dia da Instituição, contudo, ainda é necessário retê-los.

Exemplo: armazenamento de fichas com informações pessoais sobre ex-empregados(as) e ex-alunos(as).

8.6.8. **Avaliação da informação:** ato de apreciamento qualitativo do dado.

Exemplo: detectar se um dado é sensível ou não; se demanda maior segurança ou não, etc.

8.6.9. **Classificação:** ato de atribuir ao dado uma ordem, classe, gênero, espécie ou tipo, visando ordená-lo.

8.6.10. **Controle da informação:** ato de regular, determinar ou monitorar as ações sobre os dados.

Exemplo: determinar medidas de proteção sobre os dados; controlar acesso...

8.6.11. **Modificação:** ato ou efeito de alterar dados.

8.6.12. **Processamento:** ato de interpretar sistematicamente os dados, visando um resultado específico.

8.6.13. **Reprodução:** ato de copiar dados de um repositório para outro.

8.6.14. **Utilização:** ato ou efeito de se servir ou de se aproveitar dos dados armazenados.

8.6.15. **Compartilhamento:** ato ou efeito de distribuir os dados a terceiros.

Exemplo: compartilhamento de dados de empregados entre o Departamento Pessoal e Medicina do Trabalho.

8.6.16. **Comunicação:** ato ou efeito de enviar dados para um conjunto determinado de destinatários.

Exemplo01: envio de informações sociais (RAIS) e financeiras (DIRF) dos trabalhadores aos Órgãos competentes.
Exemplo02: envio de informações de alunos à Secretaria de Educação.

8.6.17. **Difusão:** ato de divulgar ou propagar dados para um conjunto indeterminado de destinatários.

8.6.18. **Distribuição:** ato de dispor dados, a partir de algum critério estabelecido, com Órgãos, Entidades, Empresas ou Prestadores de Serviços.

8.6.19. **Eliminação:** ato ou efeito de excluir ou de destruir dados armazenados ou arquivados, independentemente do procedimento empregado.

8.6.20. **Transferência:** ato de alterar o local (físico ou eletrônico) de armazenamento ou de arquivamento dos dados para outro, seja este (local) controlado pela Instituição, seja este controlado por terceiros.

8.6.21. **Transmissão:** ato ou efeito de enviar dados entre dois repositórios, por meio eletrônico.

9. Sobre o Tratamento de Dados Pessoais da Criança e do Adolescente

9.1. Além das disposições gerais que foram e ainda serão estabelecidas nesta *PIPDP*, o *tratamento* de *dados pessoais* da criança e do adolescente respeitará o que é discorrido neste Título.

9.2. O *tratamento* de *dados pessoais* de crianças e adolescentes deverá ser realizado com o consentimento específico e em destaque (**Anexo 03**), dado por pelo menos um dos pais ou pelo responsável legal devidamente identificado(s) no Contrato de Prestação de Serviços de Educação Escolar assinado.

9.3. Por sua *Política de Privacidade Institucional – PPI*, o IISNS manterá pública a informação sobre os tipos de dados pessoais coletados de crianças e adolescentes, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 da Lei nº. 13.709/2018 (LGPD).

9.4. As informações sobre o tratamento de *dados pessoais* da criança e do adolescente deverão ser publicadas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do titular, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança ou do adolescente.

10. Da Classificação dos Dados Pessoais Tratados

10.1. Os *dados pessoais* tratados pelo IISNS serão classificados de acordo com a sua natureza, sendo:

10.1.1. **Sensível:** *dado pessoal* descrito no art. 5, II da LGPD e no item **'1.1.2'** desta *PIPDP*;
10.1.2. **Comum:** *dado pessoal* que não possa ser rotulado como *sensível* (vide art. 5, I da LGPD e item **'1.1.1'** desta *PIPDP*);
10.1.3. **Anonimizado:** na forma do art. 5, III da LGPD e item **'1.1.3'** desta *PIPDP*.

10.2. Qualquer *dado pessoal* classificado como *sensível* exigirá a máxima proteção pelos *colaboradores* (*agentes internos*) do IISNS, sendo tratados estritamente nos moldes indicados pelo *Comitê de Segurança da Informação*.

11. Dos Níveis de Acesso e de Sigilo

11.1. Todo *dado* (*latu sensu*) tratado pelos *colaboradores* (*agentes internos*) do IISNS deverá ser tratado como **sigiloso**, sendo compartilhado, comunicado, difundido e/ou distribuído a qualquer outro *agente interno* ou *externo* apenas quando:

11.1.1. Expressamente autorizado por superior hierárquico; ou
11.1.2. A *operação* de tratamento de dados devidamente identificada pelo *Comitê de Segurança da Informação* assim o exigir.

11.2. Os *dados pessoais* serão tratados pelo *Setor* que instituiu a respectiva *finalidade* ou àqueles que tenham recebido autorização expressa para tanto, respeitado o *nível de acesso e de sigilo* de cada *dado pessoal*, instituído por esta *PIPDP*.

12. Da Eliminação dos Dados Pessoais

12.1. Encerrada a *finalidade* a qual o *tratamento* de *dados pessoais* está atrelado, estes (*dados pessoais*) serão eliminados dos bancos de dados físicos e eletrônicos do IISNS, salvo quando:

12.1.1. Existir previsão legal ou normativa que impeça a eliminação;
12.1.2. Existir *legítimo interesse* do IISNS para que os dados não sejam eliminados;
12.1.3. Anonimizados.

12.2. A eliminação dos *dados pessoais* do IISNS respeitará a *Tabela de Temporalidade* prevista no **Anexo 01** desta *PIPDP*.

Seção 2.Dados Pessoais Tratados em Meios Físicos

13. Conceito

13.1. Para os fins desta *PIPDP*, considera-se *dados pessoais* tratados em meios físicos aqueles (*dados*) *armazenados* ou *arquivados* em *documentos impressos* (cadernos, pastas, planilhas, dossiês e similares), aqui denominados *arquivos físicos*.

14. Dos Arquivos Físicos

14.1. O acesso ao *Setor* onde repousam os *arquivos físicos* (*armazenados* ou *arquivados*) deve ser limitado ao pessoal autorizado, cujo controle dependerá da segurança adequada.
14.2. São medidas de segurança relacionadas ao acesso à cada *Setor*:

14.2.1. Controle de entrada de pessoal;
14.2.2. Chave de acesso física ou eletrônica;
14.2.3. Restrições de acesso baseadas na *posição hierárquica* do *agente interno* (colaborador);

14.3. Os *arquivos físicos* devem ser dotados de pelo menos uma das medidas de segurança citadas no item anterior, sendo a medida mais comum o *armazenamento* em local protegido por **chave**, esta, de uso exclusivo do(s) colaborador(es) (*agente* ou *agentes internos*) de cada *Setor*.
14.4. Os *arquivos físicos* poderão ser digitalizados (*armazenados* em Meios Digitais, na forma da **Seção 3** deste Capítulo), no entanto, os *arquivos físicos* remanescentes serão eliminados apenas:

14.4.1. Mediante a autorização expressa do membro do *Comitê de Segurança da Informação* atuante na *Unidade* de origem daquele documento; ou
14.4.2. Após o encerramento do prazo previsto na *Tabela de Temporalidade* (**Anexo 01** desta *PIPDP*).

Seção 3.Dos Dados Pessoais Tratados em Meios Digitais

15. Conceito

15.1. Para os fins desta *PIPDP*, considera-se *dados pessoais* tratados em meios digitais aqueles (*dados*) *armazenados* ou *arquivados* de forma eletrônica, interligada ou não à internet (Pen Drive, CD-ROM, DVD, HD, Estação de Trabalho, Sistemas e Bancos de Dados digitais, Nuvem).

16. Do Compartilhamento de Dados Pessoais Tratados em Meios Digitais

16.1. O *compartilhamento* de *dados pessoais* tratados em meios digitais pelo IISNS se dará mediante a utilização de ***pasta*** criada para este fim no sistema de armazenamento de dados na nuvem (***drive***) utilizado pela *Unidade*.
16.2. Para os fins deste procedimento, o(a) colaborador(a) do IISNS irá:

16.2.1. Criar uma ***pasta*** no vinculada à sua *conta corporativa* (vide **'Seção 4'** deste Capítulo) para salvar o arquivo que pretende compartilhar; ou
16.2.2. Se valer de um ***drive*** previamente criado e compartilhado com o(s) destinatário(s) específico(s) do arquivo que pretende compartilhar.

16.3. O *compartilhamento* de *dados pessoais* à *agente externo* deverá ser acompanhado do *"Termo de Acesso à Pasta Compartilhada"*, conforme **Anexo 07** desta *PIPDP*, com o objetivo de informá-lo sobre as obrigações e responsabilidades para com os *dados* recebidos, em especial sobre a eliminação destes tão logo se encerre a *finalidade* do *compartilhamento*.

17. Da Política de Cookies

17.1. Os sítios eletrônicos do IISNS poderão utilizar arquivos *cookies*, com o fim de registrar e gravar, as preferências de navegação quando do acesso pelo usuário.
17.2. Os *cookies* utilizados pelo IISNS são assim classificados:

17.2.1. **Essenciais:** permitem funcionalidades essenciais, tais como segurança, verificação de identidade e gerenciamento de rede. Esses *cookies* não podem ser desativados.
17.2.2. **Marketing:** usados para rastrear a eficácia da publicidade, fornecer um serviço mais relevante e anúncios melhores para atender aos interesses do usuário.
17.2.3. **Funcionais:** coletam dados para lembrar as escolhas que os usuários fazem e para melhorar e proporcionar uma experiência mais personalizada.
17.2.4. **Analíticos:** ajudam a entender como os usuários interagem com os sítios eletrônicos da Instituição, descobrir erros e fornecer uma melhor análise geral.

17.3. A utilização dos *cookies* tem fins estatísticos e de aprimoramento dos serviços prestados pelo IISNS, devendo ser precedida do consentimento expresso do titular.
17.4. Ressalvados os *cookies* essenciais, todos os demais deverão estar marcados como "desativados" por padrão nos sítios eletrônicos do IISNS, com vista a garantir a privacidade dos usuários (titulares dos *dados pessoais* tratados).
17.5. Os sítios eletrônicos do IISNS disponibilizarão *links* para que os usuários (titulares dos *dados pessoais* tratados), possam alterar as configurações de *cookies* a qualquer momento.

Seção 4.Dos Sistemas utilizados pelo IISNS

18. Da Criação da Conta Corporativa

18.1. O colaborador (*agente interno*) do IISNS que necessitar acesso a um dos Sistemas por ele utilizados receberá uma *conta corporativa* para, além de identificá-lo nos meios digitais, possibilitar o envio e o recebimento de e-mails, bem como o armazenamento de dados na nuvem (Drive).
18.2. A *conta corporativa* do colaborador (*agente interno*) será criada pelo *Setor* de Tecnologia da Informação da *Unidade*.
18.3. Nenhum colaborador (*agente interno*) poderá compartilhar a mesma *conta corporativa* com outrem, tampouco compartilhar a senha de acesso relacionada a esta *conta*.

18.4. A abertura de uma *conta corporativa* será precedida da assinatura de Termo de Compromisso de Uso pelo colaborador (*agente interno*) que está recebendo a *conta* (**Anexo 09**).
18.5. Criada a *conta corporativa*, o *Setor* de Tecnologia da Informação encaminhará o Termo de Compromisso de Uso ao Departamento Pessoal para arquivo em local adequado.

19. Do Cancelamento da Conta Corporativa

19.1. O colaborador (*agente interno*) desligado do IISNS terá sua *conta corporativa* cancelada, no ato do desligamento.
19.2. O *Setor* de Pessoal da *Unidade* ao qual esteja vinculado um *colaborador* (*agente interno*) demitido ou afastado, deve comunicar imediatamente o responsável do *Setor* de Tecnologia da Informação da *Unidade* para as providências.

Seção 5.Do Sistema de Monitoramento por Câmeras

20. Conceitos e Definições

20.1. O IISNS se vale de *sistema de monitoramento por câmeras* com a finalidade de resguardar a segurança interna da Instituição, visando *"a proteção da vida ou da incolumidade física do titular ou de terceiros"*, nos moldes da LGPD (Lei Geral de Proteção de Dados – Lei nº. 13.709/2018).
20.2. O *sistema de monitoramento por câmeras* do IISNS poderá conter *dados pessoais* como: imagens e a respectiva data e hora exata da coleta.
20.3. Para os fins desta Seção, entende-se:

20.3.1. **dado(s)/informação(ões)/arquivo(s) do sistema:** os *dados pessoais*, incluindo as *imagens*, tratados no *sistema de monitoramento por câmeras*;
20.3.2. **sistema:** o próprio *sistema de monitoramento por câmeras*.

21. Da Guarda de dados/informações/arquivos no Sistema

21.1. Os dados/informações/arquivos gerados pelo sistema são:

21.1.1. De uso interno do IISNS, tratados apenas por pessoal autorizado à luz da sua *Política Institucional de Proteção de Dados Pessoais*.
21.1.2. Sobrescritos automaticamente pelo próprio mecanismo DVR / NVR, no prazo definido na *Tabela de Temporalidade* prevista no **Anexo 01** desta *PIPDP*, sendo irrecuperáveis após sobrescritos.

21.2. **Nenhum** dado/informação/arquivo do *sistema* será *publicado* e/ou *compartilhado* com terceiros, salvo por determinação judicial ou administrativa a ser encaminhada ao (e analisada pelo) *Comitê de Segurança da Informação*.

22. Da Solicitação de Interessados

22.1. Mediante solicitação escrita, enviada ao e-mail lgpd@redesacramentinadeeducacao.org.br, qualquer interessado poderá requerer:

22.1.1. A confirmação da existência de tratamento de dados/informações/arquivos no *sistema*;

22.1.2. A extensão do *tempo de guarda* definido nesta Política, a qual poderá ser atendida por período não superior à 150 (cento e cinquenta) dias além do habitual.

22.2. Havendo solicitação escrita do interessado, e ultrapassado o prazo de guarda e de *extensão* (**item '22.1.2'**) contados da data da *geração* ou *coleta* do dado/informação/arquivo pelo *sistema*, sem que haja determinação *judicial* ou *administrativa* que autorize o seu compartilhamento com terceiros, este (dado/informação/arquivo) será sobrescrito e, portanto, se tornará irrecuperável.

Seção 6.Dos Titulares de Dados Pessoais

23. Do Exercício dos Direitos dos Titulares

23.1. Os *titulares* de dados pessoais tratados pelo IISNS terão garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta *PIPDP* e da Lei nº. 13.709/2018 (LGPD).

23.2. O IISNS cuidará para que os *titulares* de dados pessoais por ele tratados usufruam dos direitos assegurados pela Lei nº. 13.709/2018 (LGPD), informando em sua *Política de Privacidade Institucional (PPI)* os procedimentos necessários à sua fruição.

23.3. Os pedidos dos *titulares* serão dirigidos ao *Encarregado de Dados Pessoais* (DPO), que irá registrá-los, examiná-los e respondê-los, observados os limites estabelecidos pela própria Lei nº. 13.709/2018 (LGPD) e pela legislação correlata à temporalidade de tratamento dos *dados pessoais* do solicitante.

Capítulo 4. Do Plano de Resposta a Incidentes

24. Do Comitê de Crise

24.1. O *Comitê de Crise* é formado pelos membros do *Comitê de Segurança da Informação*, e tem como atribuições:

24.1.1. Confirmar o *incidente*;
24.1.2. Mapear as dimensões do *incidente*, em especial no que tange aos *dados pessoais* e respectivos *titulares* envolvidos;
24.1.3. Prestar as orientações necessárias aos *colaboradores* (*agentes internos*) do IISNS sobre as medidas de contenção do *incidente*;
24.1.4. Analisar a possibilidade de recuperação dos *dados pessoais* envolvidos no *incidente*;
24.1.5. Identificar, coletar e preservar as evidências que tangenciam o *incidente*;
24.1.6. Elaborar comunicações aos *controladores* (nos casos em que o IISNS atuar como *operadora*) e *titulares* de *dados pessoais*, bem como à *Autoridade Nacional de Proteção de Dados* (ANPD);
24.1.7. Elaborar documentação com a avaliação interna do incidente, medidas adotadas e análise de risco, para fins de demonstração, pelo IISNS, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Art. 6º, X da LGPD);
24.1.8. Avaliar, com base em todo o arcabouço de informações relacionadas ao incidente, a necessidade de ajustes na *operação de tratamento de dados pessoais* que possam eliminar futuras ocorrências.

24.2. São indispensáveis à composição do *Comitê de Crise*:

24.2.1. O *Encarregado de Dados Pessoais* (DPO);
24.2.2. A Consultoria Jurídica da Instituição.

24.3. Além destes, o *Comitê de Crise* se valerá do auxílio de colaboradores (*agentes internos*) atuantes nos *Setores* de Tecnologia da Informação e Comunicação do IISNS.

25. Dos Incidentes Envolvendo Dados Pessoais Tratados pelo IISNS e/ou por um dos seus Operadores

25.1. O *incidente de segurança envolvendo dados pessoais*[2] tratados pelo IISNS e/ou por um dos seus *operadores* será objeto das medidas previstas neste **Capítulo**, além de outras que o *Comitê de Crise*, entender adequadas.
25.2. Qualquer *colaborador* (*agente interno*) do IISNS que identificar o *incidente de segurança envolvendo dados pessoais* deverá informar **imediatamente** o

[2] Vide item '1.1.17'.

Encarregado de Dados Pessoais (DPO) da Instituição, para que sejam tomadas as providências cabíveis.

25.2.1. A comunicação do incidente de segurança envolvendo dados pessoais será feita através do preenchimento do Relatório de Ocorrências relacionadas ao Tratamento de Dados Pessoais (**Anexo 10**).

25.2.2. Preenchido, o *Relatório de Ocorrências* deve ser encaminhado para o e-mail lgpd@redesacramentinadeeducacao.org.br.

25.3. Caso os campos (perguntas) deste *Relatório de Ocorrências relacionadas ao Tratamento de Dados Pessoais* não consigam descrever por completo a ocorrência que o *colaborador* (*agente interno*) pretende relatar, deverá ele enviar um e-mail para lgpd@redesacramentinadeeducacao.org.br com as informações mais detalhadas sobre ela (ocorrência), para que as devidas providências sejam tomadas.

25.4. São exemplos de incidente de segurança envolvendo dados pessoais:

25.4.1. O *acesso* indevido de *dados pessoais* por qualquer pessoa;

25.4.2. O *compartilhamento* de pasta contendo *dados pessoais* para outro destinatário que não pertence à *operação de tratamento* (endereço de e-mail errado);

25.4.3. O vazamento de dados pessoais por meio do *"desaparecimento"* de um *"caderno com anotações de controle de entrada, com nomes e telefones"*.

26. Da Análise e Da Avaliação dos Incidentes pelo Comitê de Crise

26.1. Identificado o *incidente de segurança envolvendo dados pessoais* pelo *Encarregado de Dados Pessoais* (DPO) da Instituição, este levará o caso **imediatamente** ao conhecimento do *Comitê de Crise* para que este possa:

26.1.1. Mitigar os eventuais *riscos* e os eventuais *danos* causados pela ocorrência;

26.1.2. Discutir as providências necessárias para corrigi-la;

26.1.3. Identificar, coletar e preservar as evidências que tangenciam o *incidente*.

26.2. Após tomadas as providências iniciais previstas no item anterior, o *Comitê de Crise* realizará a análise e a avaliação do *incidente de segurança envolvendo dados pessoais*, com o intuito de:

26.2.1. Certificar os *dados pessoais* e os *titulares* envolvidos no incidente;

26.2.2. Mensurar os eventuais *danos* causados pelo *incidente*;

26.2.3. Mensurar a *extensão* do *incidente* no tempo.

27. Dos Procedimentos a Serem Adotados pelo Comitê de Crise e demais Agentes Internos

27.1. O *Comitê de Crise* elaborará, em tempo hábil e após tomadas todas as providências destacadas anteriormente, a respectiva comunicação do *incidente de segurança envolvendo dados pessoais* aos titulares envolvidos e à ANPD.
27.2. Elaboradas as medidas de mitigação do(s) fato(s) que desencadeou(aram) o *incidente de segurança envolvendo dados pessoais*, estas serão repassadas aos *agentes internos* e *externos* do IISNS para que estes possam adequar a *operação de tratamento de dados pessoais*.

Capítulo 5. Disposições Finais e Transitórias

28. Da Revisão desta Política Institucional de Proteção de Dados Pessoais

28.1. O IISNS, por seu *Comitê de Segurança da Informação*, o qual integra o *Encarregado de Dados Pessoais* (DPO), poderá rever e alterar os termos desta *Política Institucional de Proteção de Dados Pessoais* a qualquer momento.

ANEXO 01 – Tabela de Temporalidade de Dados

Instituto das Irmãs Sacramentinas de Nossa Senhora

TEMPO E RESPONSABILIDADE DE GUARDA

ATENÇÃO: O período de guarda é sempre contado a partir de 1º de janeiro do ano seguinte à emissão (ou competência) do documento.

Nº	DOCUMENTOS ORIGINAIS	TEMPO (Anos)	RESPON-SABILIDADE	SETOR
1	Atas de Eleição de Diretorias Gerais	Indeterm.	Matriz	ADM
2	Auditagens Externas – Parecer e Documentos similares	10	Matriz	ADM
3	Bolsas CEBAS: Processos de Renovação (Desde que aquele Exercício não esteja ainda em aberto para a Concessão de CEBAS)	10	Matriz	ADM
4	Bolsas CEBAS: Relatórios de Prest. de Contas, Listagens de Bolsistas etc. (Desde que aquele Exercício não esteja ainda em aberto para a Concessão de CEBAS)	10	Matriz	ADM
5	CEBAS – Documentos para o MEC: Cópias dos Relatórios Anuais e dos docs. dos Processos de Renovação Trienal do CEBAS (Desde que aquele Processo não esteja ainda em aberto para a Concessão de CEBAS)	10	Matriz	ADM
6	Estatutos e Documentos similares	Indeterm.	Matriz	ADM
7	Veículos – Documento de Transferência (Registro)	Até a venda	Matriz	ADM
8	Contabilidade – Demonstrações Contábeis	Indeterm.	Matriz	CONT
9	Contabilidade – Livros Diários	Indeterm.	Matriz	CONT
10	Contabilidade – Livros Razão	10	Matriz	CONT
11	Contabilidade – SPED Fiscal (Sistema Público de Escrit Digital – Fiscal)	5	Matriz	CONT
12	DARFs – IRRF e outros Recolhimentos de Tributos	5	Matriz	CONT
13	Declarações Eletrônicas de Serviços/Município de Belo Horizonte – DES	5	Matriz	CONT
14	Declarações sobre Contribuições e Tributos Federais – DCTF	5	Matriz	CONT
15	Declarações sobre Retenções Federais – DIRF	5	Matriz	CONT
16	Atas de Nomeações de Diretorias das Unidades	Indeterm.	Unidade	ADM
17	Contratos Comuns, Curtos...: Locação, Prest. de Serviços Educ. e similares	5	Unidade	ADM
18	Contratos Especiais, Longos...: Locação, Prestação de Serviços e similares	Indeterm.	Unidade	ADM
19	Escrituras, Registros e Plantas de Imóveis	Indeterm.	Unidade	ADM
20	INSS – Certificado de Matrícula (Construções)	Indeterm.	Unidade	ADM
21	Orçamentos – Processos Orçamentários Anuais	5	Unidade	ADM
22	Planilhas de Custos, Cálculos de Mensalidades e similares	5	Unidade	ADM
23	Veículos – Documentos diversos após a venda	10	Unidade	ADM
24	Veículos – DPVAT, Taxa de Licenciamento e Documentos similares	5	Unidade	ADM

25	Documentos relacionados a compra de materiais e contratação de serviços: Orçamentos e similares	5	Unidade	Compras
26	Bolsas CEBAS: Documentos comprob. da Análise socioeconômica (Desde que aquele Exercício não esteja ainda em aberto para a Concessão de CEBAS)	5	Unidade	Conc. Bolsas
27	Bolsas CEBAS: Relatórios, listagens e similares (Desde que aquele Exercício não esteja ainda em aberto para a Concessão de CEBAS)	10	Unidade	Conc. Bolsas
28	Ações Judiciais, Trabalhistas e similares – Após término da Ação	10	Unidade	DP
29	CIPA – Documentos relacionados	5	Unidade	DP
30	CIPA – Livro de Atas	Indeterm.	Unidade	DP
31	Desligados(as): Passados 30 dias após o acerto rescisório, pode-se inutilizar os seguintes documentos: Protocolo de envio de arquivo; solicitação de admissão; *chek list* de admissão e demissão; cálculos rescisórios; cadastro e recadastro do/a funcionário/a; comprovante de devolução de documentos (cart. trab., por ex.); cópias da cart. de trabalho, cert. de nasc., identidade, CPF, escolaridade, endereço, atestado de antecedentes e similares	30 dias contados após o acerto rescisório	Unidade	DP
32	Desligados(as): Contrato de Experiência, Contrato por Tempo Determinado e documentos similarares (Após o desligamento)	2	Unidade	DP
33	Desligados(as): Extrato do FGTS	2	Unidade	DP
34	Estagiários(as): Todos os documentos (contado após afastamento)	1	Unidade	DP
35	FP – Acordo de Compensação de Horas	5	Unidade	DP
36	FP – Atestados Médicos para Abono de Faltas	5	Unidade	DP
37	FP – Autorização para Descontos não previstos em Lei	5	Unidade	DP
38	FP – Aviso Prévio ou Pedido de Demissão	5	Unidade	DP
39	FP – CAGED – Cadastro Geral de Empregados e Desempregados	5	Unidade	DP
40	FP – Cartões ou Livros ou Folhas de Pontos dos Empregados	5	Unidade	DP
41	FP – Contra-cheques e outros Comprov. de pagamentos a Empregados	5	Unidade	DP
42	FP – Férias: Avisos, Recibos, Solicitação e Recibo de Abonos	5	Unidade	DP
43	FP – Folhas de Pagamentos aos Empregados	35	Unidade	DP
44	FP – Folhas de Pagamentos de Serviços Prestados sem Vínculo Empregatício e respectivos Recibos e Contratos (Autônomos)	35	Unidade	DP
45	FP – GFIPs e FGTS – Documentos relacionados	35	Unidade	DP
46	FP – Horários de Trabalhos, inclusive aulas	5	Unidade	DP
47	FP – Livros ou Fichas de Registro de Empregados	Indeterm.	Unidade	DP
48	FP – Memória de Cálculos de Remuneração de Salários e Honorários	5	Unidade	DP
49	FP – RAIS (Relação Anual de Informações Sociais) – Recibos e outros Docs	5	Unidade	DP
50	FP – Recibo de Entrega do Doc. para Movimentação do Seg. Desemprego	5	Unidade	DP
51	FP – Recibos de Adiantamento de Salários	5	Unidade	DP
52	FP – Recibos de Pensão Alimentícia	5	Unidade	DP
53	FP – Rescisões de Contratos de Trabalho	35	Unidade	DP

54	FP – Rescisões Parciais de Contratos de Trabalho (Resilições)	35	Unidade	DP
55	FP – Vales Transporte – Solicitação, Recibos e similares	5	Unidade	DP
56	INSS – Acidente de Trabalho – CAT e outros Documentos	10	Unidade	DP
57	INSS – Atestados de Afastamento – Maternidade, Doenças etc.	5	Unidade	DP
58	INSS – Atestados de Escolaridade	5	Unidade	DP
59	INSS – Atestados de Vacina	5	Unidade	DP
60	INSS – Guias de Previdência Social – GPSs da respectiva Unidade	35	Unidade	DP
61	INSS – Retenções: Documentos relacionados	5	Unidade	DP
62	INSS – Salário-Família – Fichas, Termo de Responsabilidade e similares	5	Unidade	DP
63	INSS – Salário-Maternidade – Fichas, Atestados e similares	5	Unidade	DP
64	IRRF – Declaração de Dependentes	5	Unidade	DP
65	Livros de Inspeção do Trabalho	Indeterm.	Unidade	DP
66	Livros de Pontos antigos de Professores (mais de 20 anos)	Indeterm.	Unidade	DP
67	PIS – Comprovante de Cadastro	35	Unidade	DP
68	PCMSO – Programa de Controle Médico e de Saúde Ocupacional: ASOs	5	Unidade	DP
69	PCMSO – Programa de Controle Médico e de Saúde Ocupacional: Relatórios, Contratos etc.	20	Unidade	DP
70	PPRA – Programa de Prevenção e Riscos Ambientais: EPIs	5	Unidade	DP
71	PPRA – Programa de Prevenção e Riscos Ambientais: Relatórios, Contratos etc.	20	Unidade	DP
72	Sindicatos – Contribuição Sindical, Taxas Assistenciais, Relação de Empregados etc.	5	Unidade	DP
73	Sindicatos – Convenções e Acordos Coletivos de Trabalho	5	Unidade	DP
74	Ativo Imobilizado: Notas Fiscais e Documentos similares	20	Unidade	DF
75	Contabilidade – Balancetes Mensais	10	Unidade	DF
76	Contabilidade – Movimentação Bancária: Boletins, extratos, guias e similares	10	Unidade	DF
77	Contabilidade – Movimentação de Caixa: Boletins e similares	10	Unidade	DF
78	Contabilidade – Relatórios Diversos	10	Unidade	DF
79	IPTU – Guias quitadas das Taxas, com demonstração da Imunidade do Imposto	5	Unidade	DF
80	IRRF e outras Retenções de Tributos: Documentos relacionados	5	Unidade	DF
81	IRRF e outros Tributos – Recolhimento Centralizado - Impresso de Informação à Matriz	5	Unidade	DF
82	ISSQN – Imposto Sobre Serviços de Qualquer Natureza (Retenção na Fonte)	5	Unidade	DF
83	ITBI – Imposto de Transmissão de Bens Imóveis	5	Unidade	DF
84	Notas Fiscais de Compras de Produtos, Recibos Comuns, Faturas e similares	10	Unidade	DF
85	Notas Fiscais de Serviços de Pessoas Jurídicas	10	Unidade	DF
86	Receita – Comprovantes de Receitas (Mensalidades escolares etc)	10	Unidade	DF
87	Seguros Patrimoniais (Prédios, Veículos e similares) – Documentos relacionados	5	Unidade	DF

88	Taxa de Fiscalização para Funcionamento e Documentos similares	5	Unidade	DF

ANEXO 02 – Tratamentos de Dados Específicos

Tratamento	Proteção Indicada
Listas de contatos dos alunos e seus responsáveis **Listas de contatos de empregados;** **Listas de turmas;**	**Quando se Tratar de Listas Físicas** ➔ Sempre guardá-las em local fechado com chave (ex.: gaveta) quando não as estiver utilizando; ➔ Não as deixar expostas à mesa ou outro local de acesso público; ➔ Não fazer cópias da(s) lista(s), exceto quando for expressamente autorizado; ➔ Não repassar as listas ou os dados nela existentes à pessoa não autorizada (lembre-se: a lista é de uso restrito, limitado ao desenvolvimento das atividades de quem a detém); ➔ Quando substituídas, eliminá-las de forma adequada, seguindo as orientações do *Comitê de Segurança da Informação*; ➔ Não as descartar no lixo comum, especialmente antes de serem devidamente inutilizadas (terem os dados anonimizados ou rasurados). **Quando se Tratar de Listas salvas em Meio Digital** ➔ Não fazer cópias do(s) arquivo(s), exceto quando for expressamente autorizado; ➔ Não enviar as listas ou os dados nela existentes à pessoa não autorizada (lembre-se: a lista é de uso restrito, limitado ao desenvolvimento das atividades de quem a detém); ➔ Quando substituídas, eliminá-las de forma adequada, seguindo as orientações do *Comitê de Segurança da Informação*.
Envio de listas para terceiros (como em viagens);	➔ Enviar a demanda para o *encarregado de dados pessoais (DPO)* analisar a existência de cláusula(s) de *tratamento de dados pessoais* e de *confidencialidade* no contrato firmado com os terceiros (*agentes externos*) que receberão os dados; ➔ Checar a existência de consentimento prévio dos alunos e seus responsáveis para o compartilhamento; ➔ Enviar os dados apenas daqueles que consentiram o *compartilhamento*; ➔ Utilizar apenas o *canal* de *compartilhamento* previamente estabelecido pelo *Comitê de Segurança da Informação* para este fim (*link* de acesso restrito em pasta compartilhada pelo Google Drive ou One Drive, a depender da Unidade).
Utilização de WhatsApp;	➔ Não utilizar *contas pessoais* para o envio e/ou recebimento de dados pessoais; ➔ Não compartilhar dados pessoais através do WhatsApp, em especial dados pessoais sensíveis.
Recebimento de documentos de alunos/pais/responsáveis;	**Quando enviados documentos físicos**

Recebimento de documentos de empregados;	➔ Guardá-los IMEDIATAMENTE em local fechado com chave (ex.: gaveta) até o envio ao *Setor* responsável; ➔ Encaminhá-los tão logo quanto possível ao *Setor* responsável; ➔ Não fazer cópias do(s) documentos(s), exceto quando for expressamente autorizado; ➔ Não enviar quaisquer documentos ou os dados neles existentes à pessoa não autorizada. **Quando enviados em Meio Digital** ➔ Utilizar apenas o *canal* de *compartilhamento* previamente estabelecido pelo Comitê de Segurança da Informação para este fim; ➔ Deixar de receber documentos por quaisquer outros *canais* "não oficiais"; ➔ Caso os titulares assim o façam (enviem documentos por *canais* "não oficiais"), eliminá-los IMEDIATAMENTE, orientando-os sobre o meio adequado para o envio; ➔ Não fazer cópias do(s) documentos(s), exceto quando for expressamente autorizado; ➔ Não enviar/compartilhar quaisquer documentos ou os dados neles existentes à pessoa não autorizada.
Controle de entrada e saída de alunos;	➔ Coletar apenas os dados necessários para o controle de entrada e saída; ➔ Utilizar apenas o *canal* de *coleta* de informações e controle de entrada e saída (não fazer controles manuais não autorizados); ➔ Não fazer cópias do(s) controle(s), exceto quando for expressamente autorizado; ➔ Não enviar quaisquer dados sobre o controle de entrada e saída à pessoa não autorizada.
Compartilhamento interno de documentos;	➔ Utilizar apenas o *canal* de *compartilhamento* previamente estabelecido pelo Comitê de Segurança da Informação para este fim (acesso restrito em pasta compartilhada pelo Google Drive ou One Drive, a depender da Unidade); ➔ Não fazer cópias do(s) arquivo(s), exceto quando for expressamente autorizado; ➔ Não enviar quaisquer arquivos ou os dados neles existentes à pessoa não autorizada.
Compartilhamento externo de documentos;	➔ Enviar a demanda para o *encarregado de dados pessoais (DPO)* analisar a existência de cláusula(s) de *tratamento de dados pessoais* e de *confidencialidade* no contrato firmado com os terceiros (*agentes externos*) que receberão os dados; ➔ Utilizar apenas o *canal* de *compartilhamento* previamente estabelecido pelo *Comitê de Segurança da Informação* para este fim (*link* de acesso restrito em pasta compartilhada pelo Google Drive ou One Drive, a depender da Unidade); ➔ Recolher o "aceite" nos Termos de Uso da Pasta Compartilhada, na forma desta *PIPDP*.

Publicação de imagens (em geral);	➔ Checar a existência de *consentimento* prévio assinado pelo aluno e seus responsáveis; ➔ Publicar apenas fotos daqueles que consentiram o ato; ➔ Não publicar fotos de alunos cujo *consentimento* prévio não foi dado; ➔ Anonimizar eventual "foto coletiva" em que apareça, ainda que minimamente, um aluno desprovido de *consentimento*.
Cobrança de inadimplentes.	➔ Utilizar apenas os dados necessários para realizar a cobrança; ➔ Quando do envio de dados para Escritório de Cobrança de Inadimplentes: utilizar apenas o *canal* de *compartilhamento* previamente estabelecido pelo *Comitê de Segurança da Informação* para este fim (*link* de acesso restrito em pasta compartilhada pelo Google Drive ou One Drive, a depender da Unidade); ➔ Quando do envio de dados aos Órgãos de Proteção de Crédito: utilizar apenas o(s) meio(s) oficiais para o ato.

ANEXO 03 – Termo para Alunos

TERMO DE CONSENTIMENTO E AUTORIZAÇÃO

TRATAMENTO DE DADOS PESSOAIS EM RAZÃO DO CONTRATO DE PRESTAÇÃO DE SERVIÇOS EDUCACIONAIS

Pelo presente instrumento particular, o(a) aluno(a) **NOME**, inscrito(a) no CPF sob o nº. [CPF], atualmente matriculado(a) no(a) [SÉRIE/ANO], do [SELECIONAR SEGMENTO] para o ano letivo de [ANO], representado(a) ou assistido(a) por quem de direito, abaixo qualificado(s), beneficiário(a) dos serviços educacionais contratados com o **INSTITUTO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA**, pessoa jurídica de direito privado inscrita no CNPJ. sob o nº. 22.292.372/0001-25, mantenedora do(a) **[UNIDADE]**, este(a), inscrito(a) no CNPJ. sob o nº. 22.292.372/0000-00 e com endereço no(a) [RUA], nº. [Nº.], bairro [BAIRRO], CEP. [CEP.], [CIDADE] – [UF], **DECLARA**, ter ciência, consentir e autorizar que todos os dados e informações fornecidas, para a prestação e o cumprimento deste contrato educacional, serão tratados conforme as diretrizes da política adotada pela CONTRATADA, em observância às disposições contidas na Lei nº. 13.709/2020 (Lei Geral de Proteção de Dados – LGPD), nos moldes abaixo.

1. Do Consentimento/Autorização de Tratamento

1.1. Por este Termo, o(a) aluno(a), por seu(s) representante(s) ou assistente(s), manifesta o seu livre e expresso consentimento para **coleta**, **armazenamento**, **uso**, **divulgação** e **veiculação** dos seus dados pessoais, sensíveis ou não, quando necessário, diretamente ou por intermédio de terceiros (operadores ou controladores de dados pessoais), sempre em observância da legislação pertinente.

1.2. O tratamento de dados pessoais, aqui autorizado, respeitará a finalidade a qual está atrelado, como por exemplo (mas não somente):

1.2.1. Campanhas promocionais e institucionais da CONTRATADA;

1.2.2. Divulgação das atividades diversas, entre elas: pedagógicas, pastorais, recreativas e/ou comemorativas da [UNIDADE], promovidas com a participação do(a) aluno(a) representado(a) ou assistido(a), ou advindas do mérito pessoal deste;

1.2.3. Produção de materiais de uso interno da [UNIDADE], entre eles: Foto de identificação para a Ficha Cadastral; identificação facial do(a) aluno(a) representado(a) ou assistido(a); Carteirinha do(a) aluno(a) representado(a) ou assistido(a).

1.3. Os dados pessoais do(a) aluno(a) representado(a) ou assistido(a), referidos neste Termo, não poderão ser tratados em finalidade diversa daquela estabelecida no item anterior.

1.4. O(s) representante(s) ou assistente(s) legal(ais) abaixo qualificado(s) fica(m), desde já, expressa e oportunamente ciente(s) de que o tratamento dos *dados pessoais*, aqui autorizado poderá ocorrer:

1.4.1. Pelos meios de comunicação disponíveis à CONTRATADA, como: rádio, televisão, internet, redes sociais, mídia impressa (folhetos em geral, encartes, mala direta, catálogo, folder de apresentação, anúncios em revistas e jornais em geral), *outdoor*, *busdoor*, cartazes, *backlight*, mídia eletrônica (painéis, vídeo-tapes, cinema, entre outros);

1.4.2. Por intermédio de empresa parceira especializada.

1.5. Em paralelo, o(s) representante(s) ou assistente(s) legal(ais) abaixo qualificado(s) fica(m), desde já, expressa e oportunamente ciente(s) de que:

1.5.1. Os seus dados pessoais e os dados pessoais do(a) aluno(a) representado(a) ou assistido(a) poderão ser armazenados, compartilhados e utilizados para o atendimento de obrigação legal ou regulatória que a CONTRATADA tenha que cumprir, bem como para o exercício regular de seus direitos;

1.5.2. É livre para solicitar o acesso, a retificação, a supressão e a exclusão destes dados, a qualquer momento, desde que eventual solicitação não conflite com as exigências legais de órgãos educacionais, reguladores e fiscalizadores, ou impossibilitem a continuidade da prestação do serviço educacional;

1.5.3. Os seus dados pessoais e os dados pessoais do(a) aluno(a) representado(a) ou assistido(a) poderão, por força de legislação fiscal, ser transmitidos aos órgãos oficiais de fiscalização tributária que incidam sobre o presente Contrato.

2. Das Disposições Finais

2.1. O presente consentimento/autorização abrange o tratamento de dados pessoais, acima mencionado, em todo o território nacional e no exterior, podendo ser revogado a qualquer tempo por manifestação escrita do(a) titular ao *encarregado de dados pessoais* (DPO) da CONTRATADA, a ser formalizada pelo e-mail lgpd@redesacramentinadeeducacao.org.br.

E por estar(em) ciente(s) e de acordo com todas as disposições acima, o(s) representante(s) ou assistente(s) legal(ais) do(a) aluno(a) assinam este Termo para que surta os seus esperados efeitos.

[CIDADE], [DATA].

[NOME DO(A) ALUNO(A)]
CPF nº. [Nº. CPF]

[NOME DO(A) RESPONSÁVEL]
CPF nº. [Nº. CPF]

ANEXO 04 – Termo para Empregados

TERMO DE CONSENTIMENTO E AUTORIZAÇÃO

TRATAMENTO DE DADOS PESSOAIS / AUTORIZAÇÃO GRATUITA DE USO DE IMAGEM, VOZ E NOME

Pelo presente instrumento particular, o(a) Sr(a). **NOME**, inscrito(a) no CPF sob o nº. [CPF], residente e domiciliado(a) no(a) [RUA], nº. [Nº.], bairro [BAIRRO], CEP. [CEP.], [CIDADE] – [UF], nesta avença denominado(a) *"EMPREGADO(A)"*, **DECLARA** ter ciência, consentir e autorizar que todos os dados e informações fornecidas, no âmbito da relação trabalhista, serão tratados conforme as diretrizes da política adotada pelo **INSTITUTO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA**, pessoa jurídica de direito privado inscrita no CNPJ. sob o nº. 22.292.372/0001-25, mantenedora do(a) **[UNIDADE]**, este(a), inscrito(a) no CNPJ. sob o nº. 22.292.372/0000-00 e com endereço no(a) [RUA], nº. [Nº.], bairro [BAIRRO], CEP. [CEP.], [CIDADE] – [UF], em observância às disposições contidas na Lei nº. 13.709/2020 (Lei Geral de Proteção de Dados – LGPD), nos moldes abaixo.

1. Do Consentimento/Autorização de Tratamento

1.1. Por este Termo, o(a) EMPREGADO(A), manifesta o seu livre e expresso consentimento para **coleta**, **armazenamento**, **uso**, **divulgação** e **veiculação** dos seus dados pessoais, sensíveis ou não, quando necessário, diretamente ou por intermédio de terceiros (operadores ou controladores de dados pessoais), sempre em observância da legislação pertinente.

1.2. O tratamento de dados pessoais, aqui autorizado, respeitará a finalidade a qual está atrelado, como por exemplo (mas não somente):

1.2.1. Campanhas promocionais e institucionais da [UNIDADE];

1.2.2. Divulgação das atividades diversas, entre elas: pedagógicas, pastorais, recreativas e/ou comemorativas da [UNIDADE], promovidas com a participação do(a) EMPREGADO(A), ou advindas do mérito pessoal deste;

1.2.3. Produção de materiais de uso interno da [UNIDADE].

1.3. Os dados pessoais do(a) EMPREGADO(A), referidos neste Termo, não poderão ser tratados em finalidade diversa daquela estabelecida no item anterior.

1.4. O(A) EMPREGADO(A) fica, desde já, expressa e oportunamente ciente de que o tratamento dos *dados pessoais*, aqui autorizado poderá ocorrer:

1.4.1. Pelos meios de comunicação disponíveis à [UNIDADE], como: rádio, televisão, internet, redes sociais, mídia impressa (folhetos em geral, encartes, mala direta, catálogo, folder de apresentação, anúncios em revistas e jornais em geral), *outdoor*, *busdoor*, cartazes, *backlight*, mídia eletrônica (painéis, vídeo-tapes, cinema, entre outros);

1.4.2. Por intermédio de empresa parceira especializada.

1.5. Em paralelo, o(a) EMPREGADO(A) fica, desde já, expressa e oportunamente ciente de que:

1.5.1. Os seus dados pessoais poderão ser armazenados, compartilhados e utilizados para o atendimento de obrigação legal ou regulatória que a [UNIDADE] tenha que cumprir, bem como para o exercício regular de seus direitos;

1.5.2. É livre para solicitar o acesso, a retificação, a supressão e a exclusão destes dados, a qualquer momento, desde que eventual solicitação não conflite com as exigências legais de órgãos educacionais, reguladores e fiscalizadores, ou impossibilitem a continuidade da prestação do serviço educacional;

1.5.3. Os seus dados pessoais poderão, por força de legislação fiscal, ser transmitidos aos órgãos oficiais de fiscalização tributária que incidam sobre o presente Contrato.

2. Das Disposições Finais

2.1. O presente consentimento/autorização é concedida a título gratuito e abrange o uso e o tratamento dos dados pessoais acima mencionados em todo o território nacional e no exterior, podendo ser revogado a qualquer tempo por manifestação escrita do(a) titular ao *encarregado de dados pessoais* (DPO) da [UNIDADE], a ser formalizada pelo e-mail lgpd@redesacramentinadeeducacao.org.br.

E por estar ciente e de acordo com todas as disposições acima, o(a) EMPREGADO(A) assina este Termo para que surta os seus esperados efeitos.

[CIDADE], [DATA].

[NOME]
CPF nº. [Nº. CPF]

ANEXO 05 – Termo para Casa de Formação

TERMO DE CONSENTIMENTO E AUTORIZAÇÃO

TRATAMENTO DE DADOS PESSOAIS / AUTORIZAÇÃO GRATUITA DE USO DE IMAGEM, VOZ E NOME

Pelo presente instrumento particular, o Sr. **NOME**, inscrito no CPF sob o nº. [CPF], e a Sra. **NOME**, inscrito no CPF sob o nº. [CPF], residentes e domiciliados no(a) [RUA], nº. [Nº.], bairro [BAIRRO], CEP. [CEP.], [CIDADE] – [UF], nesta avença denominados ***"RESPONSÁVEIS"*** por **NOME**, inscrito(a) no CPF sob o nº. [CPF], ***"FORMANDA"***, **DECLARAM** ter ciência, consentir e autorizar que todos os dados e informações fornecidas, no âmbito da relação FORMATIVA, serão tratados conforme as diretrizes da política adotada pelo **INSTITUTO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA**, pessoa jurídica de direito privado inscrita no CNPJ. sob o nº. 22.292.372/0001-25, nome religioso, **CONGREGAÇÃO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA**, responsável pela **CASA DE FORMAÇÃO**, localizada no endereço à Rua Demétrio Ribeiro, nº. 239, bairro Vera Cruz, CEP. 30.285-680, Belo Horizonte – MG, em observância às disposições contidas na Lei nº. 13.709/2020 (Lei Geral de Proteção de Dados – LGPD), nos moldes abaixo.

1. Do Consentimento/Autorização de Tratamento

1.1. Por este Termo, os responsáveis, manifestam o seu livre e expresso consentimento para uso dos seus dados pessoais **coleta**, **armazenamento**, **uso**, **divulgação** e **veiculação**, sensíveis ou não, por exemplo, mas não somente, do seu nome, imagem e voz.

1.2. O uso/tratamento de dados pessoais, aqui autorizado, poderá ocorrer diretamente ou por intermédio de terceiros (operadores ou controladores de dados pessoais), sempre em observância da legislação pertinente, para as seguintes finalidades:

1.2.1. Participação em atividades pastorais, vocacional, encontros formativos, celebrações da Congregacional, da Conferência dos Religiosos do Brasil e outros;

1.2.2. Divulgação das atividades diversas, entre elas: serviço de animação vocacional, pastorais, recreativas e/ou comemorativas da CONGREGAÇÃO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA, promovidas com a participação da FORMANDA, ou advindas do mérito pessoal deste;

1.2.3. Produção de materiais de uso interno/externo da CONGREGAÇÃO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA.

1.3. Os dados pessoais da FORMANDA, referidos neste Termo, não poderão ser tratados em finalidade diversa daquela estabelecida no item anterior.

1.4. Os responsáveis e a FORMANDA ficam, desde já, expressa e oportunamente cientes de que o uso/tratamento dos dados pessoais, aqui autorizado poderá ocorrer:

1.4.1. Pelos meios de comunicação disponíveis à CONGREGAÇÃO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA, como: rádio, televisão, internet, redes sociais, mídia impressa (folhetos em geral, encartes, mala direta, catálogo, folder de apresentação, anúncios em revistas e jornais em geral), *outdoor*, *busdoor*, cartazes, *backlight*, mídia eletrônica (painéis, vídeo-tapes, cinema, entre outros);

1.4.2. Por intermédio de empresa parceira especializada.

1.5. Em paralelo, os responsáveis e a FORMANDA ficam, desde já, expressa e oportunamente cientes de que:

1.5.1. Os seus dados pessoais poderão ser armazenados, compartilhados e utilizados para o atendimento de obrigação legal ou regulatória que a CONGREGAÇÃO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA tenha que cumprir, bem como para o exercício regular de seus direitos;

1.5.2. É livre para solicitar o acesso, a retificação, a supressão e a exclusão destes dados, a qualquer momento, desde que eventual solicitação não conflite com as exigências legais, reguladores e fiscalizadores, ou impossibilitem a continuidade da prestação do serviço formativo para a Vida Religiosa;

1.5.3. Os seus dados pessoais poderão, por força de legislação pertinente, ser transmitidos a órgãos públicos de fiscalização.

2. Das Disposições Finais

2.1. O presente consentimento/autorização é concedido a título gratuito e abrange o uso e o tratamento dos dados pessoais acima mencionados em todo o território nacional e no exterior, podendo ser revogado a qualquer tempo por manifestação escrita do(a) titular ao encarregado de dados pessoais (DPO) da CONGREGAÇÃO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA, a ser formalizada pelo e-mail lgpd@redesacramentinadeeducacao.org.br.

E por estar ciente e de acordo com todas as disposições acima, os responsáveis e formanda assinam este Termo para que surta os seus esperados efeitos.

[CIDADE], [DATA].

[NOME DO(A) ALUNO(A)]
CPF nº. [Nº. CPF]

[NOME DO(A) RESPONSÁVEL]
CPF nº. [Nº. CPF]

[NOME DO(A) RESPONSÁVEL]
CPF nº. [Nº. CPF]

ANEXO 06 – Revogação do Consentimento

REVOGAÇÃO DE CONSENTIMENTO

PUBLICAÇÃO DE IMAGENS EM REDES SOCIAIS

Pelo presente instrumento particular, o(a) aluno(a) **NOME**, inscrito(a) no CPF sob o nº. [CPF], atualmente matriculado(a) no(a) [SÉRIE/ANO], do [SELECIONAR SEGMENTO] para o ano letivo de [ANO], representado(a) ou assistido(a) por quem de direito, abaixo qualificado(s), beneficiário(a) dos serviços educacionais contratados com o **INSTITUTO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA**, pessoa jurídica de direito privado inscrita no CNPJ. sob o nº. 22.292.372/0001-25, mantenedora do(a) **[UNIDADE]**, este(a), inscrito(a) no CNPJ. sob o nº. 22.292.372/0000-00 e com endereço no(a) [RUA], nº. [Nº.], bairro [BAIRRO], CEP. [CEP.], [CIDADE] – [UF], em observância às disposições contidas na Lei nº. 13.709/2020 (Lei Geral de Proteção de Dados – LGPD):

- ➔ **REVOGA**, nesta data, o consentimento para que sua imagem (foto) seja **publicada** em *redes sociais* pela CONTRATADA.

O(s) representante(s) ou assistente(s) legal(ais) do(a) aluno(a) assinam este Termo para que surta os seus esperados efeitos.

[CIDADE], [DATA].

[NOME DO(A) ALUNO(A)]
CPF nº. [Nº. CPF]

[NOME DO(A) RESPONSÁVEL]
CPF nº. [Nº. CPF]

ANEXO 07 – Termo de Acesso à Pasta Compartilhada

TERMO DE ACESSO À PASTA COMPARTILHADA

1. Do Acesso à Pasta Compartilhada

1.1. O **INSTITUTO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA** envia a você o *link* de uma Pasta Compartilhada através do Google Drive, cujo objetivo é permitir o seu acesso ao seu conteúdo.
1.2. A Pasta Compartilhada nesta oportunidade contém arquivos em diversos formatos, dotados de dados pessoais (sensíveis ou não) e/ou informações internas da Instituição, compartilhados unicamente para se atingir finalidade específica, inerente à Operação de Tratamento de Dados Pessoais devidamente mapeada.
1.3. Seu acesso a esta Pasta será encerrado tão logo seja atingida a finalidade correspondente ao tratamento.

2. Das Obrigações e das Responsabilidades do(a) Destinatário(a)

2.1. Ao receber este acesso, você estará obrigado a:

2.1.1. Cumprir e observar a legislação brasileira sobre privacidade e tratamento de dados pessoais e de direitos do consumidor, sobretudo aquelas estampadas:

2.1.1.1. No Marco Civil da Internet (Lei nº. 12.965/2014) e em seu Decreto Regulamentador (Decreto nº. 8.771/2016); e
2.1.1.2. Na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº. 13.709/2018).

2.1.2. Tratar todo e qualquer dado pessoal (sensível ou não) em estrita conformidade com a finalidade que se visa naquela Operação de Tratamento de Dados Pessoais.
2.1.3. Não realizar qualquer tratamento dos dados pessoais (sensíveis ou não) que seja incompatível com a finalidade da Operação de Tratamento de Dados Pessoais a que estão atrelados, como por exemplo, mas não somente:

2.1.3.1. Não produzir cópias não autorizadas dos arquivos salvos na Pasta;
2.1.3.2. Não compartilhar os arquivos salvos na Pasta à terceiros, alheios à Operação de Tratamento de Dados Pessoais a que estão atrelados.

2.1.4. Não realizar qualquer tratamento dos dados pessoais (sensíveis ou não) para além do prazo de acesso que lhe foi concedido.
2.1.5. Adotar medidas de segurança contra vazamentos e/ou acessos não autorizados, a fim de proteger os dados e informações compartilhados;

2.1.6. Comunicar imediatamente ao IISNS quando houver suspeita ou confirmação de qualquer vazamento destes dados e/ou acesso(s) indevido(s), sob pena de responder pessoalmente pelas reparações e sanções porventura causadas.

2.2. Nos termos da LGPD, em especial o disposto nos artigos 42 a 45, você é responsável por qualquer vazamento de dados pessoais a que der causa, por conta de falha de segurança nos produtos e/ou serviços contratados, devendo responder diretamente ao seu titular e/ou à autoridade ou entidade, pública ou privada, em razão de vazamentos ou danos de qualquer natureza, ficando garantido ao IISNS o direito de regresso e denunciação à lide, nos termos do artigo 125, II, do Código de Processo Civil, se porventura vier a ser demandada, a este respeito, por conduta que lhe for imputável.

3. Da Política de Privacidade

3.1. Findo o acesso à Pasta Compartilhada, você deverá excluir de seus servidores e banco de dados de forma definitiva, sem *backup* ou cópia, todos os dados pessoais (sensíveis ou não) e informações tratados ao longo da Operação de Tratamento de Dados Pessoais a que estão atrelados, certificando a exclusão destes dados por instrumento escrito, assinado por seu encarregado de tratamento de dados (D.P.O).

4. Das Disposições Finais

4.1. Ao acessar a Pasta Compartilhada você se declara ciente e de acordo com todas as disposições acima, bem como com a *Política de Privacidade Institucional* do IISNS.
4.2. Em caso de dúvidas e comunicações, contate o nosso Encarregado de Dados Pessoais, através do e-mail lgpd@redesacramentinadeeducacao.org.br.

ANEXO 08 – Termo de Compromisso para Acesso ao Sistema de Câmeras

Que entre si firmam, de um lado, o **INSTITUTO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA**, pessoa jurídica de direito privado inscrita no CNPJ. sob o nº. 22.292.372/0001-25, mantenedora do(a) **[UNIDADE]**, este(a), inscrito(a) no CNPJ. sob o nº. 22.292.372/0000-00 e com endereço no(a) [RUA], nº. [Nº.], bairro [BAIRRO], CEP. [CEP.], [CIDADE] – [UF], doravante designado *"EMPREGADOR"*, e, de outro lado, o(a) Sr(a). **NOME**, inscrito(a) no CPF sob o nº. [Nº. CPF.], portador(a) da CTPS nº. [Nº. CTPS], série [SÉRIE CTPS] – [UF], nesta oportunidade designado(a) *"EMPREGADO(A)"*:

1. Do acesso do(a) EMPREGADO(A) ao Sistema de Monitoramento por Câmeras

1.1. O(A) EMPREGADO(A) declara estar recebendo nesta data o acesso ao *sistema de monitoramento por câmeras*, sendo responsável pelo respectivo uso enquanto perdurar o seu Contrato de Trabalho.
1.2. A *conta* criada para fins de acesso ao *sistema* descrito no item anterior é de propriedade do EMPREGADOR.

2. Das Obrigações do(a) EMPREGADO(A)

2.1. O(A) EMPREGADO(A) se compromete a:

2.1.1. Acessar e utilizar o *sistema de monitoramento por câmeras* apenas para propósitos relacionados às suas atividades profissionais diárias, ficando proibido o uso para fins particulares, próprio ou de terceiros, **não podendo**, ainda:

2.1.1.1. Compartilhar e/ou emprestar sua *senha única de acesso* a terceiros;
2.1.1.2. Deixar que outras pessoas utilizem e/ou manuseiem sua *conta*, salvo quando expressamente autorizado pelo EMPREGADOR (a exemplo nos casos de manutenção de sistemas, realizada pelo *Setor* de Informática);
2.1.1.3. Produzir cópias não autorizadas dos dados/informações/arquivos gerados pelo *sistema*;
2.1.1.4. Excluir qualquer dado/informação/arquivo gerado pelo *sistema*;
2.1.1.5. Publicar e/ou compartilhar com terceiros qualquer dado/informação/arquivo gerado no *sistema*.
2.1.1.6. *Acessar* e/ou vincular esta *conta* a qualquer dispositivo de uso pessoal, restringindo estas ações aos equipamentos expressa e previamente autorizados pelo EMPREGADOR;

2.1.2. Sempre que necessário, solicitar auxílio sobre segurança na utilização do *sistema de monitoramento por câmeras* para o *Setor* de Informática de sua Unidade;

2.1.3. Comunicar imediatamente o *Setor* de Informática quando haja suspeita ou confirmação de vazamento de dados desta *conta*, em especial, mas não somente: advindo de furto ou roubo de equipamento(s) em que tenha acessado o *sistema de monitoramento por câmeras* armazenem dados/informações/arquivos ligados a ele, para que sejam tomadas as providencias cabíveis, sob pena de responder pessoalmente pelos danos porventura causados.

3. Da Política de Privacidade

3.1. Neste ato, o(a) EMPREGADO(A) toma ciência expressa de que, se desligado do EMPREGADOR, perderá imediata e completamente o acesso ao *sistema de monitoramento por câmeras*.

4. Das Disposições Finais

4.1. O(A) EMPREGADO(A) declara, formalmente, por meio deste documento, ter recebido orientações e instruções expressas acerca do uso do *sistema de monitoramento por câmeras*.

E por estarem cientes e de acordo com todas as disposições acima, as partes assinam este Termo para que surta os seus efeitos legais.

[CIDADE], [DATA].

[UNIDADE]
CNPJ. nº. 22.292.372/0000-00

[NOME]
CPF nº. [Nº. CPF]

ANEXO 09 – Termo de Compromisso para Uso de Conta Corporativa

TERMO DE COMPROMISSO

PARA USO DE CONTA CORPORATIVA e de PERFIS DE ACESSO AOS SISTEMAS

Que entre si firmam, de um lado, o **INSTITUTO DAS IRMÃS SACRAMENTINAS DE NOSSA SENHORA**, pessoa jurídica de direito privado inscrita no CNPJ. sob o nº. 22.292.372/0001-25, mantenedora do(a) **[UNIDADE]**, este(a), inscrito(a) no CNPJ. sob o nº. 22.292.372/0000-00 e com endereço no(a) [RUA], nº. [Nº.], bairro [BAIRRO], CEP. [CEP.], [CIDADE] – [UF], doravante designado *"EMPREGADOR"*, e, de outro lado, o(a) Sr(a). **NOME**, inscrito(a) no CPF sob o nº. [Nº. CPF.], portador(a) da CTPS nº. [Nº. CTPS], série [SÉRIE CTPS] – [UF], nesta oportunidade designado(a) *"EMPREGADO(A)"*:

1. Da Conta Corporativa e dos Perfis de Acesso criados para Uso do(a) EMPREGADO(A)

1.1. O(A) EMPREGADO(A) declara:

1.1.1. Ser responsável pelo uso da *conta corporativa* e dos *perfis de acesso aos sistemas corporativos* enquanto perdurar o seu Contrato de Trabalho;

1.1.2. Ter recebido os respectivos *login* e *senha* para acesso à *conta corporativa* e aos *perfis de acesso aos sistemas corporativos* nesta oportunidade.

1.2. Para os fins deste Termo, incluem-se no conceito de *conta corporativa* os sistemas de armazenamento em nuvem do EMPREGADOR (como Google e Microsoft365) e respectivo *webmail*.

1.3. A *conta corporativa* e os *perfis de acesso aos sistemas corporativos* disponibilizados para uso do(a) EMPREGADO(A) são de propriedade da EMPREGADORA.

2. Das Obrigações do(a) EMPREGADO(A)

2.1. O(A) EMPREGADO(A) se compromete a:

2.1.1. Utilizar a *conta corporativa* e os *perfis de acesso aos sistemas corporativos* apenas para o exercício de suas funções, ficando proibido o uso para fins particulares, próprio ou de terceiros;

2.1.2. **NÃO** compartilhar e/ou emprestar sua *senha única de acesso* a terceiros;

2.1.3. **NÃO** deixar que outras pessoas utilizem e/ou manuseiem sua *conta corporativa*, salvo quando expressamente autorizado pelo EMPREGADOR;

2.1.4. **NÃO** utilizar o *webmail* vinculado à *conta corporativa* para propósitos que não estejam relacionados às suas atividades profissionais diárias;

2.1.5. **NÃO** utilizar a *conta corporativa* para salvar e/ou compartilhar arquivos, informações e/ou dados pessoais de sua titularidade ou de terceiros;

2.1.6. **NÃO** vincular à *conta corporativa* qualquer site de terceiros (por exemplo, mas não somente: redes sociais e sites de e-commerce);

2.1.7. Comunicar imediatamente a Administração de sua Unidade quando suspeita ou confirmação de vazamento de dados da sua *conta corporativa* e/ou de qualquer *perfil de acesso aos sistemas corporativos*, em especial, mas não somente: advindo de furto ou roubo de equipamento(s) em que tenha efetuado *login* com a *conta corporativa* e/ou armazenem dados/informações/arquivos ligados a esta *conta*, para que sejam tomadas as providencias cabíveis, sob pena de responder pessoalmente pelos danos porventura causados.

3. Da Política de Privacidade

3.1. Ao receber a *conta corporativa* e os *perfis de acesso aos sistemas corporativos*, o(a) EMPREGADO(A) toma ciência expressa de que:

3.1.1. O EMPREGADOR poderá ter acesso integral ao conteúdo destas *contas*, como caixa de e-mail e arquivos salvos em *nuvem*;

3.1.2. Se desligado do EMPREGADOR, perderá imediata e completamente o acesso a esta *conta corporativa* e aos *perfis de acesso aos sistemas corporativos*, inclusive de todos os arquivos neles salvos.

3.2. O EMPREGADOR **não** é obrigado a fornecer *backup(s)* e/ou conceder acesso ao(à) EMPREGADO(A) sobre os dados e/ou arquivos armazenados nos repositórios Institucionais por meio da *conta corporativa* e *perfis de acesso aos sistemas corporativos* disponibilizados nesta oportunidade.

4. Das Disposições Finais

4.1. E por estarem cientes e de acordo com todas as disposições acima, as partes assinam este Termo para que surta os seus efeitos legais.

[CIDADE], [DATA].

[UNIDADE]
CNPJ. nº. 22.292.372/0000-00

[NOME]
CPF nº. [Nº. CPF]

ANEXO 10 – Relatório de Ocorrências relacionadas ao Tratamento de Dados Pessoais

O *Relatório de Ocorrências relacionadas ao Tratamento de Dados Pessoais* consiste em um Formulário Eletrônico que pode ser acessado:

- ➔ Através do link: https://forms.office.com/r/EG8ETZR6Sw;
- ➔ Apontando a câmera do seu celular para o *QR-Code*:

