

POLÍTICA DE ACESSO E UTILIZAÇÃO DO DOSSIÊ DIGITAL DE TURMA

PROJETO RGPD

Escola Básica dos 2.º e 3.º Ciclos da Torre

Câmara de Lobos, 23 de abril de 2025.

Documento Ref.	P000002
Versão:	1
Data:	23/04/2026
Autor:	Equipa RGPD/Cibesegurança ebtorre
Proprietário:	Escola Básica dos 2.º e 3.º Ciclos da Torre

Revisões - Histórico

Versão	Data	Autor da Revisão	Sumário das Alterações

Distribuição

Nome	Função
Hélder Miranda	Responsável Cibersegurança/Conselho Executivo

Aprovação

Nome	Cargo	Assinatura	Data
Hélder Miranda	Vice-Presidente Conselho Executivo		

Índice

0. INTRODUÇÃO	4
1. POLÍTICA DE ACESSO E UTILIZAÇÃO DO DDT	5

0. INTRODUÇÃO

O objetivo deste documento é definir a Política de Acesso e Utilização do Dossier Digital de Turma.

A Escola Básica dos 2.º e 3.º Ciclos da Torre (EB23Torre) possui o Dossier Digital de Turma (DDT) que reúne documentos relativos a cada turma, com o objetivo de apoiar o trabalho dos docentes, melhorar a comunicação entre intervenientes autorizados e garantir um registo estruturado e acessível de forma controlada.

Esta política define regras de acesso, utilização, armazenamento e segurança dos dados constantes no DDT.

1. POLÍTICA DE ACESSO E UTILIZAÇÃO DO DDT:

A EB23Torre definiu a seguinte **Política de Acesso e Utilização do DDT**:

- O DDT está alojado em *SharePoint/OneDrive* institucional, com permissões definidas pelo conselho executivo.
- A definição de acessos é feita de forma a permitir a garantia de segurança, proteção de dados e a continuidade dos processos de negócio.
- Apenas são armazenados os dados estritamente necessários para a continuidade do processo de negócio e a prestação dos serviços.
- O tratamento deve ser limitado ao necessário, evitando a recolha excessiva de dados.
- Todos os documentos estão organizados em pastas estruturadas por ano letivo e turma.
- Ficheiros contendo dados sensíveis (ex.: saúde, dificuldades de aprendizagem) devem estar acessíveis apenas a quem tem necessidade operacional.
- Os *Backups* são realizados regularmente pela Equipa TIC/Cibersegurança para um dispositivo externo armazenado em lugar seguro.
- A gestão de acessos ao DDT obedece ao princípio “need to know” (Conselho Executivo; Diretor de Turma; Professores da Turma; Serviços Administrativos; Técnicos Especializados).
- O acesso é feito exclusivamente através da conta institucional *Microsoft 365* fornecida pela escola;
- Todos os acessos e atividade são registados automaticamente.
- O Conselho Executivo pode auditar acessos ou ações suspeitas.
- É obrigatória a ativação de autenticação multifator (MFA).
- As sessões devem ser encerradas após uso, sobretudo em dispositivos partilhados.
- Não é permitido descarregar/partilhar ficheiros do DDT sem autorização.
- É proibido comentar ou divulgar dados de alunos em chats informais, redes sociais ou aplicações não autorizadas e utilizar o DDT para fins não pedagógicos ou fora das responsabilidades atribuídas.
- O uso indevido do DDT pode originar suspensão de acessos, processo disciplinar interno e eventual responsabilidade civil ou penal, nos termos da legislação aplicável.
- Os utilizadores do DDT devem participar em ações de formação sobre proteção de dados, boas práticas de cibersegurança e normas internas de utilização do DDT.
- Os dados não devem ser armazenados e mantidos na nuvem por mais tempo do que o necessário ao definido para as suas finalidades e prazos de conservação.
- No fim de cada ano letivo, os dados são guardados num dispositivo externo com password em lugar seguro e eliminados da nuvem.
- Em caso de acesso indevido, perda de dispositivo, suspeita de fuga de dados, o utilizador deve notificar o Conselho Executivo, a Cibersegurança e o Subinterlocutor para a proteção de dados da escola.