Política de Segurança Digital

Política de Segurança Digital da Escola

Aprender a usar a Internet
e os dispositivos digitais
em segurança e como recurso educativo

Este documento foi elaborado a partir dos modelos produzidos pelas equipas estafeta Label+ e European Schoolnet (www.eun.org) e recursos do Kent County Council.

Índice

Introdução

Atualmente a escola é um espaço digital onde a utilização da tecnologia, como computadores, tablets, telemóveis, Internet, entre outros, é cada vez mais comum, permitindo a crianças, jovens e adultos a troca de ideias, a interação social e as oportunidades de aprendizagem daí decorrentes e que apresentam enormes benefícios para todos, mas que podem por vezes trazer perigos.

O ensino online levanta, também, questões relativas à proteção de dados dos alunos, professores e outros intervenientes no processo educativo.

A utilização generalizada das tecnologias de informação e comunicação (TIC) e, nomeadamente, das plataformas online tem inúmeras vantagens, quer a nível pedagógico quer na circulação e disseminação da informação, quer nas plataformas administrativas e financeiras, contudo existe a necessidade de, no cumprimento da lei, garantir a proteção de dados dos utilizadores e dos próprios sistemas.

Para tirar o máximo partido das oportunidades que as tecnologias digitais oferecem é necessário conhecê-las e saber utilizá-las corretamente, visando proteger a confidencialidade, integridade, disponibilidade e autenticidade de documentos e dados pessoais. Assim é necessário que a escola adote políticas de utilização para a segurança digital de forma a garantir um ambiente mais seguro para todos os utilizadores, protegendo e preparando-os para os perigos que uma utilização incorreta pode acarretar, bem como garantir a integridade dos sistemas e da informação.

Todos os educadores, professores e demais trabalhadores devem, pois, ter consciência da importância das boas práticas de segurança digital, visando a educação, a proteção e a formação das crianças e dos jovens sob o seu cuidado para o correto e adequado uso das tecnologias.

Desta forma são identificados neste documento os princípios essenciais que todos os elementos da Comunidade Escolar precisam conhecer e aplicar.

Política de Segurança Digital da Escola - PSDE

A informação é um ativo dentro da escola e como tal deve estar sujeita a mecanismos de proteção que possam fazer frente a ameaças, vulnerabilidades e falhas.

A segurança da informação é assegurada através da implementação de um conjunto de controlos, que devem ser estabelecidos, implementados, monitorizados e revistos sempre que necessário.

Os objetivos da **Política de Segurança Digital** da escola são:

1. Identificar os princípios fundamentais, em relação à tecnologia de forma a garantir que a escola seja um ambiente seguro no que concerne à utilização de equipamentos e da Internet.
2. Sensibilizar todos os membros da escola sobre os potenciais riscos, bem como dos benefícios da tecnologia.
3. Permitir que todos os membros possam trabalhar com segurança e responsabilidade, com vista a um modelo comportamental positivo online, estando cientes da necessidade de gerir os seus próprios padrões e práticas ao usar a tecnologia.
4. Identificar procedimentos claros a adotar de forma a responder às preocupações de segurança online.

Âmbito de aplicação

Esta Política aplica-se a toda a comunidade educativa, órgãos de administração e gestão, pessoal docente e não docente, prestadores de serviços, visitantes, voluntários e outras pessoas que trabalham para ou prestam serviços em nome da escola, bem como alunos e pais/ encarregados de educação.

Esta Política aplica-se a todos os dispositivos de acesso à Internet e utilização de dispositivos de comunicação e informação, ou outros que tenham sido fornecidos a alunos, pessoal docente e não docente ou outras pessoas.

Este documento foi elaborado em consonância com a Política Geral de Proteção de Dados Pessoais para a Administração Pública da Região Autónoma da Madeira (RGPD-DOC-05-2) que tem o intuito de assegurar, na Administração Pública Regional (APR), um nível coerente e elevado de proteção dos dados pessoais das pessoas singulares, direito esse que deve ser ponderado e equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade de acordo com a legislação em vigor.

Esta PSDE, redigida com base nas diretrizes disponibilizadas pela iniciativa europeia, *Esafety Label* e na legislação aplicável, será revista, quando necessário

1. Utilização da Internet

Devendo fazer parte integrante dos processos de aprendizagem como uma ferramenta essencial, a utilização da Internet deve elevar os padrões educativos, promover o sucesso dos alunos, apoiar o trabalho dos professores e da administração escolar.

1. O acesso à Internet é um direito de toda a comunidade educativa, salvaguardando o cumprimento de normas na sua utilização.
2. Nas atividades de ensino e aprendizagem dever-se-á ensinar aos alunos a utilizar a internet de forma respeitável e segura.
3. A cópia e a utilização subsequente de materiais obtidos na Internet, por professores e alunos, devem cumprir a legislação, em matéria de direitos de autor, incluindo o conhecimento dos vários tipos de licenciamentos disponíveis e as regras de utilização dos recursos educativos abertos.
4. Todas as atividades escolares que impliquem o uso da Internet devem integrar a apresentação das referências bibliográficas.
5. Os alunos devem aprender como indicar as fontes das informações utilizadas e a respeitar os direitos de autor quando utilizam material obtido na Internet nos seus trabalhos escolares.

2. Segurança/Gestão dos sistemas de informação

2.1 Manutenção da segurança

2.1.1 A capacidade e o funcionamento dos sistemas informáticos serão analisados, pelo menos, trimestralmente.

2.1.2 A proteção antivírus será atualizada, bem como o sistema operativo ou outros programas instalados, com a periodicidade indicada no número anterior.

2.1.3 A instalação de software é realizada pelo Técnico de Sistemas e Tecnologias de Informação ou Coordenador TIC, quando se trate de equipamentos para uso pedagógico, e Coordenadores dos Manuais Digitais, quando se trate de equipamentos do Projeto Manuais Digitais.

2.1.4 A instalação de software nos laboratórios de informática pode ser realizada pelos docentes do grupo de Informática o qual deve ser reportado ao Delegado de Disciplina e Coordenador TIC.

2.1.5 Os dispositivos estão protegidos por sistemas de segurança físico, nomeadamente palavras-passe.

2.1.6 Todos os dispositivos têm uma conta de Administrador à qual só acede o Técnico de Sistemas e Tecnologias de Informação.

2.1.7 Os dados associados à administração escolar/serviços administrativos são protegidos através de um sistema de backup automatizado da responsabilidade do Técnico de Sistemas e Tecnologias de Informação.

2.1.8 Os dispositivos existentes para fins pedagógicos possuem uma segunda conta de Administrador/Professor, com acesso restrito ao Técnico de Sistemas e Tecnologias de Informação, Coordenador TIC e docentes do grupo disciplinar de Informática.

2.1.9 Nos laboratórios de Informática, a usar para disciplinas específicas de Informática, serão criadas, no início de cada ano letivo ou semestre, contas por turma, com palavra-passe, gerida pelo respetivo professor. No final de cada aula é obrigatório terminar a sessão.

2.1.10 As configurações dos equipamentos nos laboratórios de Informática e outros espaços utilizados pelos alunos são previamente definidos (Personalização do Fundo, Cores e Temas, configurações do Rato (opções do ponteiro).

2.1.11 A *Cloud Computing* para armazenamento e partilha de ficheiros é o OneDrive institucional.

2.1.12 Os dispositivos amovíveis deverão ser utilizados apenas em situações pontuais.

2.2 Gestão do correio eletrónico (e-mail)

2.2.1 Todos os docentes, não docentes e alunos devem utilizar o correio eletrónico institucional (@EDU), sendo este o meio utilizado para o envio de toda a informação institucional.

2.2.2 A comunicação com alunos, pais/ encarregados de educação e com instituições para tratamento de assuntos oficiais da escola deve ser realizada apenas a partir do correio eletrónico institucional.

2.2.3 O reencaminhamento de mensagens em cadeia, nomeadamente a divulgação de informações, ações de formação, entre outras, deve ser apenas realizada pelo Conselho Executivo e órgãos de gestão intermédia.

2.2.4 Os destinatários das mensagens do ponto anterior, não devem responder a todos os destinatários. No caso de esclarecimento de dúvidas, devem ser dirigidas apenas ao remetente.

2.2.5 A conta institucional deve ser utilizada apenas para fins pedagógicos e administrativos.

2.3 Gestão dos conteúdos publicados

2.3.1 As informações de contacto nas plataformas online devem ser: a morada, os números de telefone e o email institucional.

2.3.2 Nomes completos não são usados junto a fotografias ou gravações áudio e/ ou vídeo, de forma a reduzir a possibilidade de identificação dos alunos.

2.3.3 Não são publicadas online: pautas, horários das turmas, listagem dos alunos e das turmas, sendo apenas afixado em papel no interior da Escola nos locais de eleição, conforme o permitido e determinado por lei.

2.3.4 Todas as publicações online devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

2.3.5 As publicações na página e redes sociais da escola apenas podem ser feitas pelo coordenador TIC, embora, pontualmente, possam ser feitas pelo coordenador das atividades de enriquecimento curricular, no caso das redes sociais, quando se trate de eventos públicos ou conferências.

2.3.6 A gestão das plataformas PLACE e outras de âmbito administrativo e financeiro são da responsabilidade dos detentores dos respetivos direitos, à exceção das palavras-passe dos utilizadores que as deverão as alterar, pelo menos, semestralmente.

2.4 Publicação de trabalhos de alunos, imagem, áudio e vídeos

2.4.1 Antes da publicação de imagens ou de gravações áudio e/ou vídeo que incluam alunos, deve ser garantida a autorização expressa e informada, de acordo com a legislação aplicável, pelo encarregado de educação (Anexo 4).

2.4.2 Essa autorização é concedida, por escrito, pelos encarregados de educação, no ato da matrícula, a qual é guardada no dossier da turma pelo respetivo diretor de turma (findo o ano letivo essa autorização é arquivada no processo do aluno).

2.4.3 Os trabalhos dos alunos devem conter uma ficha técnica, na qual pode estar incluída uma licença de publicação, a qual pode ser obtida pelo endereço https://creativecommons.org/.

2.4.4 A captação de imagens dos alunos deve, preferencialmente, ser executada de longe ou de ângulos que reduzam significativamente a possibilidade de identificação dos mesmos e também deve evitar imagens com alunos de forma individual.

2.4.5 No caso de frequência dos alunos num projeto específico, onde haja a produção e publicação online de imagens ou de gravações contendo a sua voz e imagem, deve o professor responsável, obter uma autorização específica por escrito, para a sua frequência/participação neste tipo de projeto, do aluno e/ou encarregado de educação (Anexo 5).

2.4.6 Os professores não podem publicar imagens ou outros registos dos alunos nas suas redes sociais pessoais.

2.4.7 Os alunos e funcionários, também, não podem publicar nas suas redes sociais imagens recolhidas no interior da escola, que contenham imagens, trabalhos, dados pessoais dos de alunos professores e funcionários.

2.5 Gestão de comunidades sociais virtuais, redes sociais e publicações pessoais

2.5.1 A equipa de promoção da literacia digital, em consonância com o Coordenador TIC e/ou o grupo de Informática prestarão apoio, produção de conteúdos, sessões de esclarecimento, formações e/ou Workshops (mediante disponibilidade e interesse) para auxiliar e dotar os professores sobre práticas seguras de utilização da Internet.

2.5.2 Os professores que pretendam utilizar ferramentas online com os alunos em atividades curriculares devem avaliar o risco dos sítios na Internet, antes de os utilizar e verificar os termos e condições dos mesmos, de modo a garantir que são adequados às idades dos alunos.

2.5.3 A página Web da escola terá uma área de sensibilização para o uso seguro da Internet e disponibilizar aos pais/encarregados de educação materiais relacionados com o tema.

2.6 Plataformas de e-learning

2.6.1 A plataforma de *e-learning* a ser utilizada pela escola é o Microsoft Teams.

2.6.2 As equipas no Teams devem ser criadas, respeitando as regras, conforme o documento próprio da escola (Anexo 6).

2.7 Gestão dos sistemas de filtragem

2.7.1 Para aceder à rede escolar nos Polos da Calheta e Fajã, será necessário a autenticação.

2.7.2 A rede escolar é composta por três redes distintas:

- ***guest***, a ser utilizada por alunos, pessoal não docente e pessoas externas à Escola nos seus dispositivos pessoais. A palavra-passe deve ser solicitada ao diretor de turma no caso dos alunos e encarregados de educação e aos restantes visitantes à telefonista

- ***Manuais Digitais***, a ser utilizada por alunos e professores afetos ao projeto;

- ***escolar***, a ser utilizada pelo pessoal docente, pelos serviços administrativos.

As palavras-passe das redes WIFI *guest* e escolar, serão renovadas 3 dias após o final de cada semestre.

2.7.3 A gestão das palavras-passe da rede Manuais digitais é gerida pelos serviços especializados da Direção Regional de Educação.

2.7.4 A escola possui uma Firewall física gerida por uma equipa da Divisão de Tecnologias, Segurança e Infraestruturas (DTSI), da Direção de Serviços de Tecnologias e Ambientes Inovadores de Aprendizagem (DSTAIA), da Direção Regional da Educação (DRE).

2.7.5 Conforme seja necessário, serão feitas verificações para comprovar a eficácia dos métodos de filtragem implementados, através da análise de relatórios, gerados pela firewall, pela equipa da DTSI.

2.7.6 O acesso à Internet pelos equipamentos do projeto Manuais Digitais, na rede destinada aos mesmos, contém sistemas de filtragem específicos (*GlobalProtect*), gerido pela equipa dos Manuais Digitais da DTSI.

2.7.7 O acesso à Internet através das redes WiFi, destinada ao pessoal docente, não docente e visitantes, é gerido por uma firewall física, com regras distintas, sendo estas também gerida pela equipa DTSI.

2.7.8 No âmbito do projeto Manuais Digitais existem coordenadores na escola, responsáveis pela gestão do mesmo, servindo de ponte entre a escola e a DRE.

2.7.9 Os professores que utilizam esta rede, podem pedir que certos sítios na Internet sejam bloqueados ou desbloqueados, conforme a necessidade.

2.7.10 A escola toma todas as precauções possíveis para garantir que os utilizadores acedam apenas a conteúdo digital apropriado. No entanto, devido à natureza global e diversidade disponível nas redes, nem sempre é possível evitar, atempadamente, o uso indevido. Todos os membros da Comunidade Escolar que violarem os sistemas de filtragem ou acederem a sítios com conteúdos inadequados ao espaço escolar serão alvo de procedimento disciplinar, de acordo com o Estatuto do aluno, Regulamento interno da escola, Estatuto da Carreira Docente da RAM e Lei Geral de Trabalho em Funções Públicas.

3. Decisões quanto às Políticas

3.1 Autorização do acesso à Internet

3.1.1 Os pais/encarregados de educação devem ter conhecimento da Política de Segurança Digital (PSDE – **Alunos**, anexo 1 e analisá-lo com os seus filhos ou educandos.

3.1.2 No ato da matrícula, os encarregados de educação são informados da existência desta política, disponível na página Web da Escola.

3.1.3 Ao considerar o acesso para os membros vulneráveis da comunidade (como por exemplo as crianças com necessidades educativas) a escola tomará as decisões com base nas necessidades específicas e compreensão do(s) aluno(s).

3.2 Resolução de incidentes relativos à Segurança Digital

3.2.1 Todos os elementos da Comunidade Escolar devem informar o Conselho Executivo caso tenham conhecimento de situações preocupantes, do ponto de vista da segurança digital (tais como violações do sistema de filtragem, *Ciberbullying*, conteúdos ilícitos, utilização inadequada de equipamento, entre outros).

3.2.2 A escola gere os incidentes relacionados com a segurança digital em conformidade com as políticas da escola em matéria de disciplina/conduta, e, quando necessário, o Conselho Executivo, reportará os incidentes às autoridades competentes, o que não invalida a informação os encarregados de educação.

3.2.3 Todos os incidentes devem ficar registados, em documento próprio, nomeadamente o *Registo Sumário de Ocorrência* (disponível na Página Web).

3.3 Gestão de telemóveis e equipamentos pessoais

3.3.1 Os telemóveis ou equipamentos pessoais **não podem** ser utilizados durante as aulas ou tempos letivos formais (devendo, por isso, estar desligados), a não ser para efeitos pedagógicos devidamente autorizados, orientados e supervisionados pelo professor, conforme consta do RI (Artigos 7.º e 8.º).

3.3.2 Os utilizadores são responsáveis por qualquer tipo de dispositivos eletrónicos que tragam para a escola, que desassocia qualquer responsabilidade pela perda, roubo ou dano de tais objetos.

3.3.3 Os pais/encarregados de educação não devem contactar os filhos/educandos para os telemóveis durante o horário letivo. Em caso de necessidade de contacto urgente devem usar o número de telefone da escola.

3.3.4 Se um aluno necessitar de contactar os pais/encarregado de educação, deve contactar através do seu telemóvel, em período não letivo e fora de espaços como salas de aula, biblioteca, zonas comuns dos blocos e outros espaços onde possa perturbar o funcionamento dos serviços.

3.3.5 Os professores não devem utilizar os seus telemóveis ou equipamentos pessoais para contactar crianças ou jovens dentro ou fora da escola na sua qualidade de profissionais, a não ser em situações devidamente justificadas e quando outros meios de contacto não estejam operacionais. Sempre que for necessário contactar alunos ou pais/encarregados de educação, deverão usar um telefone ou os meios de comunicação oficiais da escola.

3.3.6 A captura de imagem e/ou vídeo deverá ser feita, sempre que possível, com equipamentos disponíveis na escola. Estas capturas não devem ser mantidas por um período superior a três dias, para respeitar a proteção de dados pessoais.

3.3.7 Os alunos devem proteger os seus números de telefone, dando-os a conhecer apenas a amigos e familiares de confiança.

3.3.8 Os alunos serão instruídos quanto à utilização segura e adequada de equipamentos pessoais e serão sensibilizados para os limites e consequências dos seus atos.

4. Conhecimento das políticas

4.1 Conhecimento das políticas pelo pessoal docente, não docente, alunos e pais/ encarregados de educação

4.1.1 A PSDE está disponível, para conhecimento e consulta, na página Web da Escola.

4.1.2 A Escola informará os pais/encarregados de educação da sua PSDE, através de boletins informativos e nas reuniões regulares a realizar com os diretores de turma/titulares de turma.

4.1.3 Os alunos serão informados através do diretor de turma/titular de turma da existência desta Política.

Disposições finais

Todo o pessoal em desempenho de funções nesta escola deve orientar a sua atuação respeitando os princípios da proporcionalidade e da não discriminação, na perspetiva do interesse das crianças e jovens, avaliando constantemente os riscos e o impacto que a disponibilização de dados pessoais online pode ter na vida de todos. Devem ainda, através do exemplo, sensibilizar para a necessidade de proteger os dados pessoais e respeitar a privacidade de todos e de cada um, em particular das crianças e jovens.

Todos os elementos da escola deverão estar sensibilizados para o facto de que a sua conduta online fora da escola pode afetar as suas funções e a sua reputação dentro desta.

Legislação base

- Decreto Legislativo Regional n.º 21/2013/M, de 25 de junho - Estatuto do Aluno e Ética Escolar na RAM.

- Deliberação n.º 1495/2016, de 6 de setembro - Comissão Nacional de Proteção de Dados. Disponível em https://www.cnpd.pt/media/qaxbr1y2/del_1495_2016_dados_alunos_internet.pdf, consultado a 23 de novembro de 2023.

- Lei n.º 58 /2019, de 08 de agosto – Lei da Proteção de Dados Pessoais. Disponível em https://www.pgdlisboa.pt/leis/lei_mostra_estrutura.php?tabela=leis&artigo_id=3118A0002&nid=3118&nversao=&tabela=leis&so_miolo=, consultado a 23 de novembro de 2023.

- Lei nº 59/2019, de 08 de agosto – Dados Pessoais para a prevenção, deteção, investigação ou repressão de infrações penais. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_estrutura.php?tabela=leis&artigo_id=3123A0001&nid=3123&nversao=&tabela=leis&so_miolo=?area=Identifica%E7%E3o%20civil%20e%20criminal, consultado a 23 de novembro de 2023.

- Política Geral de Proteção de Dados Pessoais para a Administração Pública da Região Autónoma da Madeira (RGPD-DOC-05-2), junho de 2022. Disponível em https://pfp.madeira.gov.pt/documentos/RGPD_DOC_05_2_Politica_de_Protecao_de_Dados_Pessoais_GRM_v1_0_signed_1116700.pdf, consultado a 23 de novembro de 2023.

Sítios na Internet

- Sítio da comissão nacional da proteção de dados: https://www.cnpd.pt/
- Direitos de autor: https://www.erc.pt/pt/legislacao/direito-de-autor-e-direitos-conexos/
- Criação de licenças: https://creativecommons.org/
- Centro Internet Segura: https://www.internetsegura.pt/
- Centro de Sensibilização SeguraNet: https://seguranet.pt/
- Selo de Segurança Digital: http://www.esafetylabel.eu/

Calheta, 29 de novembro de 2023

O Presidente do Conselho Executivo

José Bernardo Ferreira Gouveia

Parecer favorável do Conselho Pedagógico - 30 de novembro de 2023

Parecer favorável do Conselho Administrativo – 05 de dezembro de 2023

Política aprovada pelo Conselho da Comunidade Educativa - 23 janeiro de 2024

O Presidente do Conselho da Comunidade Educativa

António Manuel Ribeiro Calado

Anexos

Anexo 1 – PSDE – Alunos

Política de Segurança Digital

(alunos)

Tendo em vista o estabelecimento de práticas eficazes de utilização das Tecnologias de Informação e Comunicação (TIC) para fins de ensino e aprendizagem, torna-se fundamental que os alunos adquiram "capacidades de literacia digital".

Assim, e consciencializados para a necessidade de uma utilização adequada das TIC, quando usufruem da rede ou equipamento da escola, ou se encontram em sítios da Internet relacionados, de algum modo, com esta, fisicamente dentro ou fora da escola, os alunos estão comprometidos a:

1. Utilizar, em tempo de aulas, as TIC da escola, para fins escolares e apenas quando, devidamente, autorizados pelos professores.

2. Não navegar, fazer *download*, *upload* ou partilhar material que possa ser considerado ofensivo ou ilegal, comunicando, de imediato, ao professor se, acidentalmente, se deparar com esse tipo de material.

3. Não fornecer nenhuma informação pessoal, como nome, número de telefone ou endereço, palavra-passe, nem marcar encontros com alguém, a menos que isso faça parte de um projeto escolar aprovado pelo respetivo professor.

4. Garantir que a sua atividade *online* não desrespeite ou ofenda de algum modo a escola, os docentes e não docentes, colegas ou outros.

5. Comunicar, por intermédio das TIC, com alunos, professores ou outras pessoas de modo responsável, respeitoso e sensato, sendo responsável pela correção do comportamento ao utilizar a Internet, incluindo os sites a que acede e a linguagem que utiliza.

6. De acordo com o *Regulamento Interno* da escola não deve trazer equipamentos tecnológicos, correndo o risco de serem danificados ou roubados e não poder responsabilizar a instituição a não ser a si próprio.

7. No caso de trazer consigo o telemóvel ou outro equipamento deve desligar ou mantê-lo em modo de "silêncio", a comunicação Bluetooth e WiFi deve estar "desligada". Não deve utilizar dispositivos informáticos que possam interferir com o funcionamento das atividades letivas.

8. Não é permitida a publicação de fotos não autorizadas de colegas, pessoal docente e não docente ou outros membros da Escola, o mesmo se aplica a vídeo e áudio, bem como documentos afixados na escola que contenha informação pessoal de colegas, professores ou funcionários.

9. Caso seja vítima de *Cyberbullying,* ou tenha conhecimento que alguém que o seja, é dever e obrigação informar um professor, funcionário ou Conselho Executivo.

10. Respeitar os direitos de propriedade intelectual, tendo em conta os direitos de autor e ter sempre o cuidado de referir as fontes em todos os documentos/trabalhos produzidos.

11. Não fazer *download* ou instalar software em equipamento eletrónico escolar, nem quando acede à rede escolar, através de dispositivo próprio.

12. Após a utilização de um equipamento eletrónico escolar, todos os ficheiros devem ser removidos.

13. Deve terminar todas as sessões nas aplicações utilizadas na escola (como é exemplo o email institucional e plataforma Teams). O mesmo deve ser feito no equipamento eletrónico da escola a que aceda.

14. Utilizará a Internet respeitando os filtros existentes e as regras gerais definidas, sabendo que essa utilização é monitorizada pelos responsáveis da rede.

15. Compreender que as regras foram criadas para sua segurança e que será responsabilizado e penalizado, em caso de transgressão, sendo informado o respetivo encarregado de educação.

16. Em caso de dúvidas, procurar informar-se, junto dos professores ou através de sítios adequados, como por exemplo:

https://www.internetsegura.pt/

https://seguranet.pt/

http://www.esafetylabel.eu/

https://www.cnpd.pt/

Anexo 2 – PSDE – Docentes

Política de Segurança Digital

(pessoal docente e não docente)

É importante que todo o pessoal docente e não docente adote, dentro do possível, todas as medidas necessárias para proteger os sistemas de dados e de informação contra riscos de infeção por vírus, acesso não autorizado, danos, perdas, abusos e roubo.

Todo o pessoal docente e não docente tem a responsabilidade de usar os sistemas informáticos da escola de forma legal, ética e profissional.

Compreendendo que os Sistemas de Informação (SI) e as Tecnologias de Informação e Comunicação (TIC) incluem as redes, os dados e o seu armazenamento, as tecnologias de comunicação digital *online* e *offline* e os dispositivos de acesso, estão comprometidos a:

1. Utilizar os SI da Escola de forma adequada, conscientes de que, ao abrigo da lei portuguesa e das diretivas europeias, os seguintes atos constituem uma infração punível por lei:

- **a.** obter acesso não autorizado a material informático;
- **b.** obter acesso não autorizado a material informático com o intuito de cometer ou facilitar outros atos ilícitos;
- **c.** alterar material informático sem autorização.

2. Servir-se de todos os equipamentos e programas informáticos, disponibilizados pela escola, para fins relacionados com a mesma, evitando o acesso não autorizado a sistemas ou a dados pessoais, eliminando do "**ambiente de trabalho os seus documentos**" e terminar sessão ou encerrar o dispositivo.

3. Respeitar o sistema de segurança e não divulgar qualquer palavra-passe ou informação de segurança.

4. Não instalar qualquer software adquirido ou descarregado, quando tal seja necessário, deve pedir permissão ao Coordenador TIC.

5. Assegurar que os dados pessoais de alunos, professores ou pais/encarregados de educação são protegidos, de acordo com a legislação em vigor, nomeadamente, no que diz respeito à forma como estes são obtidos, processados, mantidos, transferidos, acedidos e utilizados.

6. Utilizar imagem, áudio e/ou vídeos de alunos com autorização prévia dos encarregados de educação.

7. Não guardar ficheiros digitais profissionais que contenham informações pessoais ou sensíveis relacionados com a escola (incluindo documentos, imagens, vídeos, etc.), em qualquer dispositivo (como computadores portáteis, discos, câmaras digitais, etc.), salvo se estiverem devidamente protegidos do acesso não autorizado, roubo e uso fraudulento, recorrendo, sempre que possível, à "*nuvem*" da sua conta

@EDU institucional (*OneDrive*), salvaguardada por palavra-passe segura, para a criação, transferência e arquivo de ficheiros digitais.

8. Respeitar os direitos de propriedade intelectual, bem como direitos de autor e mencionar sempre as suas fontes em qualquer documento.

9. No caso do pessoal docente, supervisionar os alunos na sala de aula e em outros espaços da escola, tendo em atenção à utilização de meios tecnológicos, garantindo a adequada utilização. Verificar no final da aula que os alunos terminaram sessão nas suas contas institucionais e no equipamento, quando utilizam dispositivos eletrónicos da escola.

10. Reportar ao órgão de gestão, Coordenador TIC e/ou equipa de promoção da Literacia Digital, qualquer incidente preocupante relativo à segurança dos alunos na utilização das TIC, qualquer suspeita de existência de vírus ou outro *malware* num dispositivo ou sistema e qualquer perda de ficheiro digital ou informação relacionada com a escola.

11. Utilizar as TIC e os SI (da escola ou pessoais) em consonância com as suas funções profissionais, incluindo-se a utilização de redes sociais, jogos, publicações digitais e outros dispositivos ou sítios Web.

12. Não criar, transmitir, apresentar, publicar ou encaminhar qualquer material suscetível de assediar, ofender, causar incómodo ou ansiedade desnecessários a qualquer pessoa, ou que possa trazer descrédito para a profissão, para a escola ou para a Administração Pública.

13. As comunicações eletrónicas com os alunos e pais/encarregados de educação serão realizadas exclusivamente através de canais de comunicação aprovados pela escola.

14. O pessoal docente deve promover a segurança digital junto dos alunos, ajudando-os a desenvolver uma atitude responsável quando usam sistemas informáticos e acedem à Internet relativamente aos conteúdos que criam e visualizam, ensinando-os a questionar aquilo que pesquisam e a saber retirar a informação correta, antes de a aceitar como certa.

15. O pessoal docente deve incentivar os alunos a respeitar os direitos de autor, propriedade intelectual e referir sempre as suas fontes em todos os trabalhos/documentos produzidos.

16. Estas políticas aplicam-se igualmente na utilização de equipamento pessoal na rede da escola.

17. Se tiver dúvidas ou perguntas relacionadas com práticas seguras e profissionais na Internet, deve procurar ou solicitar esclarecimento com o Coordenador TIC.

Anexo 3 – PSDE – Visitantes

Política de Segurança Digital

(visitantes)

Enquanto visitantes na Instituição, é importante que adotem, dentro do possível, todas as medidas necessárias para proteger os sistemas de informação (SI) contra acesso não autorizado, danos, perdas, abusos e roubo de informação. Assim, compreendendo que os SI e as Tecnologias de Informação e Comunicação (TIC) incluem as redes, os dados e o seu armazenamento, as tecnologias de comunicação digital *online* e *offline* e os dispositivos de acesso (são exemplos os telemóveis, as câmaras digitais, o correio eletrónico (email) e os sites de redes sociais), estão comprometidos a:

1. Os SI da escola devem ser utilizados de forma adequada. Tendo conhecimento de que, ao abrigo da lei portuguesa e das diretivas europeias os seguintes atos constituem uma infração punível por lei:

- **a.** obter acesso não autorizado a material informático;
- **b.** obter acesso não autorizado a material informático com o intuito de cometer ou facilitar outros atos ilícitos;
- **c.** alterar material informático sem autorização.

2. No caso de empréstimo de equipamentos eletrónicos estes devem ser devolvidos no período indicado e nas mesmas condições em que lhe foram entregues.

3. Pode aceder à rede sem fios da escola, nos Polos da Calheta e Fajã, por solicitação direta e conforme definido na Política de Segurança Digital da escola.

4. Não instalar qualquer software adquirido ou descarregado, sem permissão do Órgão de Gestão.

5. Assegurar que os dados pessoais de alunos, ou pais/encarregados de educação são tratados de acordo com a legislação nacional, no que diz respeito à proteção de dados pessoais.

6. Respeitar os direitos de autor e propriedade intelectual.

7. Reportar qualquer incidente preocupante relativo à segurança na Internet ao Órgão de Gestão, assim que possível.

8. Não criar, transmitir, apresentar, publicar ou encaminhar qualquer material suscetível de assediar e ofender alunos, pais/encarregados de educação, professores, ou que possa trazer descrédito para a escola.

9. Estas políticas aplicam-se igualmente na utilização de equipamento pessoal na rede da escola.

10. Se tiver dúvidas ou perguntas relacionadas com práticas seguras e profissionais na Internet, deve procurar ou solicitar esclarecimento com a escola pessoalmente ou através do email.

Anexo 4 – PSDE – Autorização de captação/ publicação de imagem e trabalhos escolares

Declaração de captação/ publicação de imagem e trabalhos escolares

Nome do aluno: _____

Nome do Encarregado de Educação: _____

A Escola Básica e Secundária com Pré-Escolar da Calheta, procede à captação e respetiva difusão da imagem dos seus alunos e divulgação de trabalhos escolares, através da sua página Web e das suas redes sociais, atendendo que são salvaguardados os cuidados necessários, descritos na Política de Segurança Digital da Escola, para fins exclusivamente de atividades de ensino e divulgação de atividades.

Tomei conhecido da Política de Segurança Digital da Escola e:

☐ **Autorizo a captação e respetiva difusão da imagem e trabalhos escolares.**

☐ **Não autorizo a captação e respetiva difusão da imagem e trabalhos escolares.**

Para o ano escolar de 20___/ 20___.

Assinatura do Encarregado de Educação

_____

Tomei conhecimento

___ / ___ / 20 ___

Recebido por:

_____

(Nome legível)

Declaração de captação/ publicação de imagem e trabalhos escolares

Nome do aluno: _____

Nome do Encarregado de Educação: _____

A Escola Básica e Secundária com Pré-Escolar da Calheta, procede à captação e respetiva difusão da imagem dos seus alunos e divulgação de trabalhos escolares, através da sua página Web e das suas redes sociais, atendendo que são salvaguardados os cuidados necessários, descritos na Política de Segurança Digital da Escola, para fins exclusivamente de atividades de ensino e divulgação de atividades.

Tomei conhecido da Política de Segurança Digital da Escola e:

☐ **Autorizo a captação e respetiva difusão da imagem e trabalhos escolares.**

☐ **Não autorizo a captação e respetiva difusão da imagem e trabalhos escolares.**

Para o ano escolar de 20___/ 20___.

Assinatura do Encarregado de Educação

_____

Tomei conhecimento

___ / ___ / 20 ___

Recebido por:

_____

(Nome legível)

Anexo 5 – PSDE – Autorização de recolha de imagem, som e vídeo para projetos e ou atividades

Declaração de autorização captação e publicação de imagem, som e vídeo para projetos e ou atividades

Projeto/ Atividade: _____ (indicar o nome do projeto/atividade)

Eu,_____, encarregado de educação do aluno(a) _____, nº ____, do ano_____º, turma_____, declaro que autorizo o meu educando(a) a participar no projeto de complemento do currículo/atividade _____, sob a orientação do professor _____.

Declaro ainda, autorizar a captação, tratamento e respetiva difusão da imagem/som e vídeo do meu educando, atendendo que serão salvaguardados os cuidados necessários, descritos na Política de Segurança Digital da Escola, para fins exclusivamente de atividades de ensino, através dos canais de comunicação da Escola e participação em concursos escolares, para o ano escolar 20___/20___.

Horário: Especificar o horário semanal do projeto

Assinatura do Encarregado de Educação

_____

Assinatura do professor:

_____

Tomei conhecimento

___ / ___ / 20 ___

Anexo 6 – PSDE – Estrutura e organização das equipas na Plataforma Teams

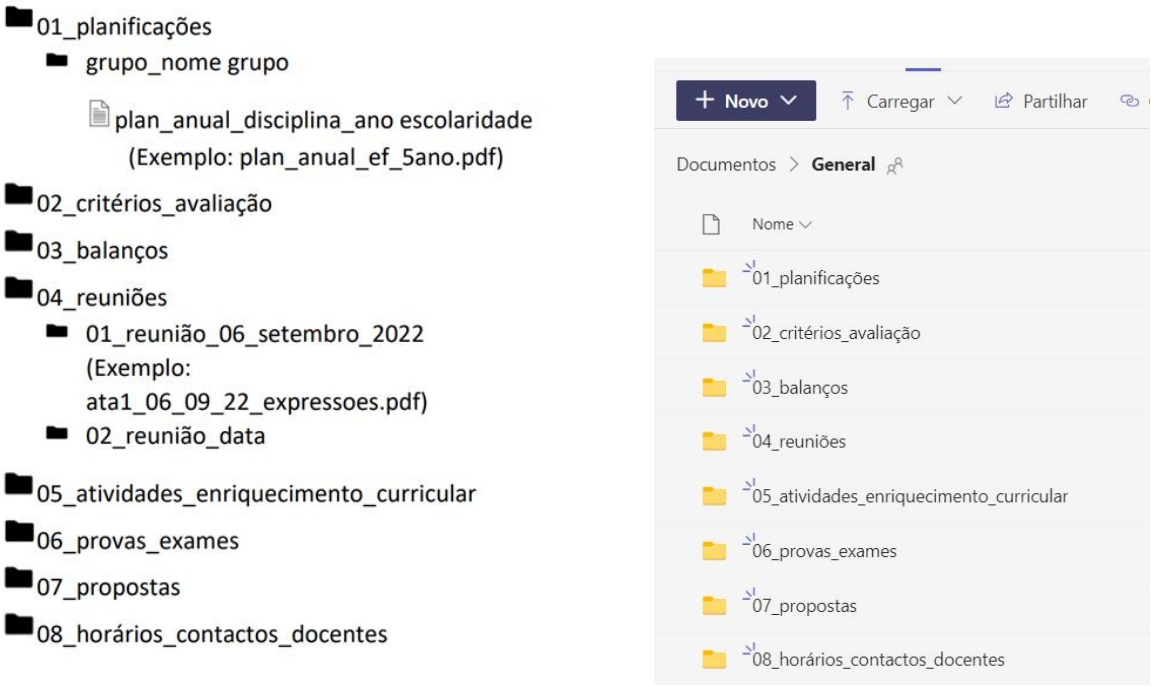
De forma a uniformizar e padronizar um conjunto de procedimentos, em particular a criação e organização das equipas na plataforma Teams, cada docente responsável pela criação de equipas deve seguir as seguintes regras:

A - Coordenador de Departamento

- Cada Coordenador de Departamento deverá criar uma equipa do tipo **PLC**, privada, no Microsoft Teams para o quadriénio;

- O nome da equipa deverá respeitar o seguinte formato, exemplo: **departamento Expressões 22-26 EBSPE Calheta**;

- No início de cada ano letivo, no separador Ficheiros, deverá criar um conjunto de pastas e subpastas com a seguinte estrutura e atribuir os nomes indicados para os ficheiros:



- No final de cada ano letivo, deverá criar uma pasta nomedepartamento_anoletivo (expressões2022_2023) e mover todas as pastas para o seu interior.

B - Delegado

- Cada delegado deverá criar uma equipa do tipo **PLC,** privada, no Microsoft Teams para o quadriénio;

- O nome da equipa deverá respeitar o seguinte formato, exemplo: **grupo Matemática 22-26 EBSPE Calheta**;

- No início de cada ano letivo, no separador Files, deverá criar um conjunto de pastas e subpastas com a seguinte estrutura, e atribuir os nomes indicados para os ficheiros:

regimento_interno.pdf

01_planificações

plan_anual_disciplina_ano escolaridade (Exemplo: plan_anual_ef_5ano.pdf)

02_critérios_avaliação

03_balanços

04_reuniões

1_reunião_06_setembro_2022

2_reunião ...

05_atividades_enriquecimento_curricular

06_partilha_recursos

07_provas_exames

08_propostas

09_horários_contactos_docentes

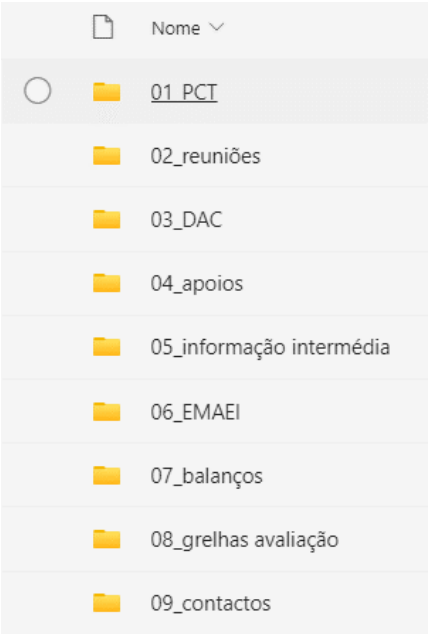
- No final de cada ano letivo, deverá criar uma pasta nomegrupo_anoletivo (matemática2022_2023) e mover todas as pastas para o seu interior.

C - Diretor de Turma

- Cada Diretor de Turma deverá criar uma equipa do tipo **PLC**, privada, no Microsoft Teams;

- O nome da equipa deverá respeitar o seguinte formato, exemplo: **CT 7º1 22-23 EBSPE Calheta**;

- No separador Files, deverá criar um conjunto de pastas e subpastas com a seguinte estrutura:



D – Professor

- Cada professor deverá criar uma equipa por disciplina/ turma do tipo **turma**, no Microsoft Teams;

- O nome da equipa deverá respeitar o seguinte formato: **7º1 Português 22-23 EBSPE Calheta**;

- No separador Files, dentro da pasta **Material de Aula**, deverá criar uma pasta para cada período/ semestre/ módulo/ UFCD;

- Cada projeto/ apoio deverá ter uma equipa no Microsoft Teams de forma a comunicar e gerir as atividades/ apoios com os seus alunos.

- Findando o ano letivo, as equipas criadas para uso com os alunos, devem ser eliminadas.