2025

2026

Política de Utilização Aceitável
PUA

Índice

Siglas e Abreviaturas

DRE – Direção Regional de Educação

DSTAIA – Direção de Serviços de Tecnologias e Ambientes Inovadores de Aprendizagem

DTSI – Direção de Tecnologias, Segurança e Infraestruturas

Escola – Escola Básica e Secundária /PE da Calheta

PUA – Política de Utilização Aceitável

TIC – Tecnologias de Informação e Comunicação

VPN – Virtual Private Network (Rede Privada Virtual)

Termos e Definições

2FA / MFA - é um método de segurança que exige mais do que uma senha para aceder a uma conta, combinando diferentes fatores.

Antispam - Ferramenta ou tecnologia que bloqueia emails indesejados ou publicitários.

Antivírus - Programa que deteta, previne e remove vírus e outros softwares maliciosos.

Blacklists - Listas de endereços, IPs ou domínios bloqueados por serem considerados perigosos ou indesejados.

Denial-of-Service (DoS) - Ataque que torna um serviço ou sistema indisponível ao sobrecarregá-lo com pedidos.

Firewall - Sistema de proteção que controla o tráfego de rede, bloqueando acessos não autorizados.

Keyloggers - Software ou hardware que regista as teclas pressionadas pelo utilizador, podendo roubar informações sensíveis.

MAC Address Spoofing - Técnica que altera o endereço MAC de um dispositivo para enganar redes ou sistemas de segurança.

Malware - Software malicioso criado para danificar, invadir ou controlar dispositivos e redes.

Scans automáticos - Processos automáticos de verificação de sistemas ou redes para detetar vulnerabilidades ou ameaças.

01 | Introdução

A Escola Básica e Secundária/PE da Calheta disponibiliza um conjunto de serviços de rede e eletrónicos com o objetivo de apoiar os processos de ensino/aprendizagem, acesso à informação e comunicação interna e externa. A utilização desses serviços está alinhada com o Regulamento Interno (RI) e os valores definidos no Projeto Educativo de Escola (PEE).

A infraestrutura de comunicações da Escola é composta por redes internas interligadas entre si e com acesso à Internet, permitindo uma rede robusta e segura que suporta atividades pedagógicas, administrativas e de gestão.

Atualmente, a escola é um espaço digital onde o uso da tecnologia – como computadores, Tablets, Chromebooks, telemóveis e a Internet – é cada vez mais comum. Este uso proporciona à comunidade educativa oportunidades de aprendizagem, interação social e troca de ideias. Contudo, também acarreta riscos relacionados com a segurança e a privacidade dos dados.

A utilização generalizada das TIC e plataformas digitais traz inúmeras vantagens, mas exige o cumprimento rigoroso da legislação vigente para garantir a proteção dos dados dos utilizadores e a integridade dos sistemas.

Para beneficiar plenamente das tecnologias digitais, é necessário compreendê-las e usá-las corretamente, respeitando os princípios da confidencialidade, integridade, disponibilidade e autenticidade da informação. Assim, torna-se essencial que a Escola adote políticas claras que promovam um ambiente seguro e protetor para todos os utilizadores.

Todos os educadores, professores e demais trabalhadores devem estar conscientes da importância das boas práticas de segurança digital. Cabe-lhes educar, proteger e formar os alunos no uso correto das tecnologias, contribuindo para a sua literacia digital e cidadania responsável.

Desta forma, este documento identifica os princípios essenciais que todos os elementos da Comunidade Escolar devem conhecer e aplicar.

A informação é um ativo fundamental da Escola e, como tal, deve ser protegida através de mecanismos que enfrentem ameaças, vulnerabilidades e falhas. Esta segurança é garantida mediante a implementação de controlos contínuos, que devem ser estabelecidos, monitorizados e atualizados sempre que necessário.

Objetivos da Política:

- Identificar os princípios fundamentais para garantir um ambiente seguro no uso da tecnologia e da Internet.
- Sensibilizar todos os membros da comunidade educativa para os riscos e benefícios do uso da tecnologia.
- Promover uma utilização segura e responsável, baseada em práticas positivas e conscientes.

02 | Enquadramento Legal

Esta política foi elaborada com base na legislação portuguesa e europeia em vigor, nomeadamente:

- Lei n.º 58/2019 (Lei da Proteção de Dados Pessoais)
- Lei n.º 59/2019 (Tratamento de dados para fins de segurança)
- Lei n.º 109/2009 (Criminalidade informática)
- Política Geral de Proteção de Dados Pessoais para a Administração Pública da Região Autónoma da Madeira (RGPD-DOC-05-2)
- Código Civil, Artº 79º
- Diretrizes da equipa Ciber.EDU.

03 | Pressupostos

Esta política tem como objetivo estabelecer os princípios orientadores da utilização adequada e responsável dos recursos e sistemas informáticos e redes de comunicações.

Aplica-se a toda a comunidade educativa, incluindo órgãos de administração e gestão, pessoal docente e não docente, prestadores de serviços, visitantes, voluntários e outras pessoas que trabalhem ou prestem serviços em nome da escola, bem como alunos e pais/encarregados de educação. É igualmente aplicável a formandos, colaboradores, parceiros e convidados.

Abrange todos os dispositivos de acesso à Internet e de utilização de tecnologias de comunicação e informação, independentemente de terem sido fornecidos pela Escola ou de serem propriedade dos utilizadores, sempre que utilizados no contexto das atividades escolares.

Todos os intervenientes educativos devem estar conscientes da sua responsabilidade ao utilizar os sistemas informáticos da Escola. Este uso deve ser legal, ético e profissional, adotando sempre medidas necessárias para proteger os sistemas e dados contra acesso não autorizado, danos, perdas, abusos e roubo.

Este documento foi elaborado em consonância com a legislação em vigor e será revisto sempre que necessário, à luz da evolução tecnológica e legislativa.

04 | Âmbito de Aplicação

4.1 Infraestrutura de comunicações com fios e sem fios

Os recursos computacionais ligados à infraestrutura de comunicações são componentes tecnológicos e sistemas que permitem a operação, gestão e suporte das redes de comunicação. Estes recursos são fundamentais para garantir que a transmissão de dados ocorra de maneira eficiente, segura e confiável.

4.2 Recursos computacionais ligados à infraestrutura de comunicações

Os recursos computacionais ligados à infraestrutura de comunicações são variados e essenciais para suportar a operação de redes de comunicação. Englobam hardware, software, e serviços que juntos asseguram a transmissão, gestão, segurança, e armazenamento de dados, permitindo que a instituição opere de maneira eficiente e segura.

4.3 Portal Institucional e plataformas de *backoffice* de apoio aos processos da atividade:

O Portal institucional é um website mantido pela instituição, que tem como objetivo fornecer informações, serviços e recursos aos seus diferentes públicos, nomeadamente, pessoal docente, não docente, discentes, Encarregados de Educação, Comunidade Educativa.

As **plataformas de *backoffice*** são sistemas internos utilizados pela Escola para gerir e suportar os processos administrativos e operacionais. São fundamentais para a eficiência e a eficácia das operações diárias.

Portal institucional disponibilizado pela Escola:

- Página Web da Escola: https://escoladigital.madeira.gov.pt/ebspecalheta

Plataformas de backoffice:

- Plataforma de gestão de assiduidade – Itime

- Plataforma de gestão de horários – Untis - Inforários
- Plataforma ENES
- Plataforma ENEB
- Plataforma PAEB

4.4 Acesso a serviços eletrónicos externos, efetuados a partir das redes de comunicações da Escola

Refere-se à capacidade de os utilizadores dentro da instituição escolar utilizarem a rede de comunicação interna da Escola para acederem a serviços e recursos disponíveis fora da infraestrutura da Escola.

Esses serviços externos podem incluir uma ampla variedade de recursos eletrónicos e plataformas baseadas na internet.

Serviços eletrónicos externos utilizados pela Escola:

- Portal Base;
- Plataforma GD – Gestão de Documentos
- Portal da CGD;
- Portal do Millennium BCP;
- Plataforma SIGORAM – Sistema de informação de gestão Orçamental;
- Portal da CGA;
- Portal da ADSE;
- Portal da Segurança Social;
- Portal AGIR;
- Portal do Funcionário Público - PFP;
- Plataforma do Tribunal de Contas;
- Plataforma do Portal das Finanças;
- Plataforma de Contratação Pública – AcinGov;
- Plataforma GESEDU – Manuais escolares;
- Sistema Integrado de Apoio à Gestão – SIAG;
- Plataforma PLACE;
- Plataforma PLAC;
- Microsoft 365
- Escola Virtual
- Aula Digital

Com / de acesso remoto:

- Plataforma TAB-POS;
- Plataforma de gestão de assiduidade – Itime;

4.5 Serviços para Comunicação, Colaboração e Armazenamento

Os serviços utilizados pela escola para comunicação, colaboração e armazenamento de documentos são o Microsoft Outlook, OneDrive e Teams, disponibilizados pela SRE a todo o pessoal docente, não docente e aos discentes, garantindo acesso seguro e integrado às ferramentas digitais da instituição.

05 | Normas Gerais

1. A informação disponibilizada pelos serviços eletrónicos, da qual a Escola é proprietária ou depositária legal, deve ser utilizada e processada em conformidade com a legislação em vigor, nomeadamente no que respeita aos direitos de autor, à proteção de dados e demais legislação aplicável.
2. O acesso à informação disponibilizada pelos serviços eletrónicos deve ser realizado de acordo com as permissões atribuídas pela Escola a cada membro da comunidade escolar.
3. Cada utilizador é responsável por comunicar de imediato qualquer desaparecimento, violação de segurança ou roubo da informação acessível.
4. A informação retirada dos serviços eletrónicos pela comunidade escolar, no âmbito das suas atividades e para equipamentos da sua responsabilidade, deve ser protegida e utilizada nos termos do ponto 1. Após a sua utilização, a informação copiada deve ser eliminada dos equipamentos.
5. Não é permitida a utilização da infraestrutura de comunicações da Escola para fins comerciais ou, de forma geral, para qualquer finalidade que não esteja alinhada com a missão e atividades institucionais da Escola.
6. Os serviços de rede e os serviços eletrónicos disponibilizados pela infraestrutura da Escola não podem ser cedidos, alugados ou vendidos a terceiros, por qualquer serviço, unidade orgânica ou utilizador individual.

7. Em casos excecionais, e mediante autorização prévia do Conselho Executivo, poderá ser concedido acesso a terceiros, nomeadamente instituições do sistema de ensino, ciência, tecnologia e cultura, com as quais a Escola mantenha protocolos de colaboração.

8. A utilização dos serviços de rede e eletrónicos para fins pessoais só é permitida se não causar degradação do desempenho dos serviços, não implicar custos adicionais e não interferir com o seu uso institucional. Em qualquer circunstância, a utilização para fins pessoais tem prioridade inferior, reservando-se a Escola o direito de a limitar ou interromper.

9. As credenciais de acesso (nome de utilizador e palavra-passe) são pessoais e intransmissíveis. Cada utilizador deve assegurar a confidencialidade das suas credenciais e adotar práticas de segurança, nomeadamente a utilização de palavras-passe seguras e, sempre que possível, autenticação multifator (MFA).

10. Os dispositivos utilizados para aceder à infraestrutura de rede da Escola devem estar atualizados e protegidos com medidas de segurança adequadas, incluindo software antivírus e *firewall*.

11. A utilização dos serviços eletrónicos deve observar princípios de ética digital. É proibida a divulgação de conteúdos ofensivos, discriminatórios ou que atentem contra os direitos de outros membros da comunidade escolar, bem como qualquer uso que comprometa a integridade, segurança ou reputação da instituição.

06 | Restrições

1. Não é permitida a extração ou transferência de informação confidencial da Escola para o exterior, por qualquer meio eletrónico, sem autorização prévia do Conselho Executivo. O incumprimento poderá implicar procedimento disciplinar e/ou criminal.

2. Durante a utilização dos serviços de rede e eletrónicos da Escola, é expressamente proibido:

    a. Qualquer atividade considerada ilegal nos termos da legislação portuguesa;

    b. Pesquisa ou exploração de vulnerabilidades nos sistemas da Escola, incluindo a utilização de ferramentas automatizadas para identificação de portas abertas, serviços ativos ou falhas de segurança (“scans automáticos”);

    c. Tentativas de acesso não autorizado a sistemas internos ou externos à Escola;

d. Qualquer tentativa de interrupção de serviços, como ataques de negação de serviço ("*Denial-of-Service*");

e. Distribuição intencional, ou por negligência, de software malicioso (*malware*) que afete o funcionamento de outros utilizadores, dentro ou fora da Escola;

f. Alteração ou falsificação de endereços físicos de rede ("*MAC Address Spoofing*");

g. Falsificação de endereços de hardware ou outras formas de manipulação de identidade digital.

3. O acesso à rede escolar nos Polos da Calheta e Fajã requer autenticação.

4. A rede escolar está dividida em três segmentos distintos:

a. ***guest*** - destinada a alunos, pessoal não docente e visitantes que utilizem dispositivos pessoais. A palavra-passe deve ser solicitada ao Diretor de Turma (no caso dos alunos e encarregados de educação) ou à telefonista (para visitantes);

b. **Manuais Digitais** - a ser utilizada pelos equipamentos afetos ao projeto;

c. **Escolar** - reservada ao pessoal docente e aos serviços administrativos.

5. As palavras-passe das redes *guest* e Escolar são renovadas no início de cada semestre.

6. A gestão das palavras-passe da rede Manuais Digitais é da responsabilidade dos serviços especializados da Direção Regional de Educação (DRE).

7. A Escola dispõe de uma firewall física gerida pela equipa da Divisão de Tecnologias, Segurança e Infraestruturas (DTSI), da Direção de Serviços de Tecnologias e Ambientes Inovadores de Aprendizagem (DSTAIA), da DRE.

8. Qualquer acesso não autorizado aos serviços de rede e eletrónicos da Escola constitui uso indevido e poderá originar procedimento disciplinar e/ou criminal.

9. Em contexto de trabalho remoto, não é permitido o acesso à rede da Escola através de ligações não seguras ou não confiáveis (por exemplo, redes Wi-Fi públicas).

10. A utilização de VPN para acesso remoto aos servidores da Escola só pode ser feita mediante autorização do Conselho Executivo e deve respeitar as mesmas boas práticas de segurança aplicáveis ao trabalho presencial.

11. A ligação de computadores pessoais à rede por cabo só é permitida com autorização prévia do Conselho Executivo e após a respetiva configuração pelos Técnicos de Sistemas de Tecnologias de Informação da Escola.

12. O equipamento eletrónico pertencente à Escola destina-se exclusivamente a atividades institucionais e pedagógicas. É proibida a sua utilização por terceiros não autorizados (por exemplo: filhos, amigos).

07 | Segurança

1. Os equipamentos ligados à infraestrutura de comunicação da Escola, utilizados para aceder aos serviços de rede e eletrónicos, devem estar protegidos contra ataques informáticos (ex.: antivírus, *firewall*). A proteção antivírus, o sistema operativo e outros programas instalados são atualizados mensalmente.

2. A instalação de software é da responsabilidade dos Técnicos de Sistemas e Tecnologias de Informação ou do Coordenador TIC, no caso de equipamentos para uso pedagógico, e dos Coordenadores dos Manuais Digitais, no caso de equipamentos integrados no Projeto Manuais Digitais.

3. Os dispositivos estão protegidos por sistemas de segurança física, nomeadamente palavras-passe.

4. Todos os dispositivos têm uma conta de Administrador, à qual apenas os Técnicos de Sistemas e Tecnologias de Informação têm acesso.

5. Os dispositivos destinados a fins pedagógicos possuem uma segunda conta de Administrador/Professor, com acesso restrito aos Técnicos de Sistemas e Tecnologias de Informação e aos docentes do grupo disciplinar de Informática.

6. As configurações dos equipamentos nos laboratórios de Informática e noutros espaços utilizados pelos alunos, são previamente definidas (ex.: personalização do fundo, cores e temas, configurações do rato – opções do ponteiro).

7. Nos laboratórios de Informática, utilizados para disciplinas específicas de Informática, são 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.

8. Os dispositivos amovíveis devem ser utilizados apenas em situações pontuais.

9. O utilizador de um equipamento informático ligado à infraestrutura da Escola deve garantir que este não é temporariamente abandonado sem estar bloqueado com uma palavra-passe e estar configurado para desencadear automaticamente o encerramento da sessão.

10. O utilizador deve garantir que a sua conta institucional de acesso aos serviços de rede e eletrónicos possui uma palavra-passe com um elevado nível de complexidade. Esta palavra-passe nunca deve ser transmitida a terceiros.

11. O utilizador deve assegurar que, no momento de introdução da palavra-passe para autenticação nos serviços, se encontra resguardado de forma a evitar que terceiros a possam observar.

12. Após utilizar os serviços de rede e eletrónicos, deve ser sempre realizada a operação de terminar sessão (*logout*) na aplicação, seguida do seu encerramento (ex.: navegadores utilizados para acesso a portais).

13. Deve ser evitado, sempre que possível, o acesso aos serviços de rede e eletrónicos da Escola a partir de equipamentos públicos cuja fiabilidade não possa ser facilmente comprovada (devido ao risco de software malicioso, como *keyloggers*).

14. No início de cada ano letivo, as contas de utilizador e e-mail de antigos colaboradores são desativadas. Após um período considerado adequado, essas contas são eliminadas.

15. O acesso aos servidores e bastidores da Escola é restrito ao pessoal autorizado, nomeadamente aos Técnicos de Sistemas e Tecnologias de Informação e à Equipa de Cibersegurança, e deve estar sempre condicionado por chave de segurança.

16. Os utilizadores não devem instalar extensões, complementos ou plugins nos navegadores sem autorização prévia dos Técnicos de Sistemas e Tecnologias de Informação, de forma a evitar riscos de segurança.

17. As sessões iniciadas em plataformas digitais da Escola não devem ser partilhadas com outros utilizadores, mesmo que pertençam à mesma turma, grupo ou equipa.

18. A partilha de ficheiros entre utilizadores deve ser feita, através das plataformas institucionais, como o OneDrive, garantindo rastreabilidade e proteção dos dados.

19. As credenciais de acesso (nome de utilizador e palavra-passe) devem ser alteradas sempre que exista suspeita de que possam ter sido comprometidas.

20. Os dispositivos portáteis (ex.: portáteis, tablets, Chromebooks) fornecidos pela Escola devem ser utilizados exclusivamente para fins educativos e não devem ser emprestados ou utilizados por terceiros sem autorização.

21. Sempre que houver suspeita de violação de segurança (ex.: acesso não autorizado, roubo de dados, perda de dispositivo), o utilizador deve comunicar imediatamente o incidente à equipa de Cibersegurança através de formulário próprio.

08 | Serviço de correio eletrónico

1. A caixa de correio eletrónico EDU atribuída a qualquer membro da comunidade escolar é considerada institucional, devendo ser utilizada exclusivamente para a transmissão oficial de informações e outras comunicações no âmbito da atividade escolar (apenas para fins pedagógicos e/ou administrativos).

2. É da responsabilidade de cada utilizador manter a confidencialidade da sua conta de correio eletrónico, não devendo partilhar as suas credenciais com terceiros, mesmo que pertençam à mesma unidade orgânica.

3. O acesso ao correio eletrónico institucional deve ser feito a partir de dispositivos confiáveis e redes seguras, evitando o uso de equipamentos públicos ou redes Wi-Fi abertas.

4. A caixa de correio institucional não deve ser utilizada para fins comerciais ou para qualquer outro fim que possa pôr em causa o bom nome da Escola.

5. Todos os docentes, não docentes e alunos devem utilizar o correio eletrónico institucional, sendo este o meio definido para o envio e receção de informação oficial.

6. A comunicação com alunos, pais/encarregados de educação e instituições, no tratamento de assuntos oficiais da Escola, deve ser realizada apenas através do correio eletrónico institucional.

7. A Escola nunca solicita, por email, telefone ou qualquer outro meio, as credenciais de autenticação (ex.: palavra-passe).

8. A caixa de correio eletrónico tem capacidade limitada, sendo da responsabilidade do utilizador a realização de manutenção periódica (ex.: arquivo ou eliminação de mensagens), de forma a garantir a sua plena operacionalidade.

9. Não devem ser enviadas mensagens para um elevado número de destinatários internos e/ou externos. Esta prática pode levar ao bloqueio do sistema de correio eletrónico da Escola por sistemas *antispam*, ao colocá-lo em listas negras (*blacklists*).

10. O reencaminhamento de mensagens em cadeia, incluindo divulgação de informações, ações de formação e outros conteúdos, deve ser feito apenas pelo Conselho Executivo ou pelos órgãos de gestão intermédia.

11. Em resposta a mensagens de correio eletrónico de cariz geral, deve evitar-se a opção "Responder a todos", de forma a não gerar comunicações em massa desnecessárias.

12. A abertura de mensagens e anexos provenientes de endereços desconhecidos deve ser evitada, por se tratar de um dos meios mais comuns de disseminação de vírus, *malware* e ataques de *phishing*. Sempre que se detete uma situação suspeita, esta deve ser reportada à Equipa de Cibersegurança através de formulário próprio. Em seguida, deve clicar-se com o botão direito na mensagem, denunciar como *phishing*, bloqueá-la e eliminá-la.

13. Deve-se ter em atenção que "CC" (*Carbon Copy*) é utilizado para dar conhecimento de uma mensagem, sendo os destinatários visíveis entre si.

14. Deve-se ter em atenção que "BCC" (*Blind Carbon Copy)* também serve para dar conhecimento, mas oculta os destinatários entre si.

15. A conta de correio eletrónico institucional deve ser protegida com uma palavra-passe robusta, única e atualizada regularmente, sendo obrigatória a utilização da autenticação de dois fatores (MFA).

16. Em caso de cessação de funções, os utilizadores devem cessar imediatamente o uso da conta de correio eletrónico institucional, a qual será desativada e, posteriormente, eliminada pelos serviços competentes.

09 | Plataforma de Ensino e Trabalho Colaborativo

1. A plataforma adotada pela Escola é o Microsoft Teams.

2. Durante sessões síncronas em plataformas de ensino a distância, é proibida a gravação, partilha de imagem ou som, sem consentimento explícito, bem como garantir que os alunos não ligam a câmara ou microfone sem necessidade pedagógica.

3. Os utilizadores devem manter uma postura adequada utilizando linguagem apropriada, evitando distrações digitais e respeitando as normas de participação definidas pelo docente.
4. As equipas criadas no Microsoft Teams devem respeitar as normas definidas (ver Anexo 1).

10 | Gestão de Conteúdos

10.1 Publicação de Conteúdos Institucionais

a. As informações de contacto divulgadas nas plataformas online da Escola devem limitar-se à morada, números de telefone e endereço de correio eletrónico institucional.

b. Não são publicadas online pautas, horários das turmas, listagens de alunos ou distribuição de turmas. Estas informações são afixadas em papel, nos locais definidos dentro da Escola, conforme permitido por lei.

c. Os nomes nunca deverão ser completos e deve ser evitada a sua utilização, bem como a identificação da turma e do número de aluno, em conjunto com fotografias ou gravações de áudio e/ou vídeo, de forma a reduzir a possibilidade de identificação.

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

e. As publicações na página web da Escola e nas redes sociais da Escola são da responsabilidade do Coordenador TIC. Pontualmente, o Coordenador das Atividades de Enriquecimento Curricular poderá também publicar conteúdos nas redes sociais, desde que relacionados com eventos públicos ou conferências.

f. A gestão das plataformas PLACE e outras de natureza administrativa ou financeira é da responsabilidade dos respetivos administradores. As palavras-passe de acesso são da responsabilidade dos utilizadores, devendo ser alteradas, no mínimo, semestralmente.

g. Todos os conteúdos publicados nas plataformas digitais da Escola devem ser revistos previamente quanto à sua exatidão, clareza e adequação, antes da sua divulgação ao público.

10.2 Trabalhos de Alunos, Imagem, Áudio e Vídeo

a. A publicação de imagens ou gravações de áudio e/ou vídeo que incluam alunos requer autorização expressa e informada do respetivo encarregado de educação, de acordo com a legislação em vigor (ver Anexo 2).

b. No âmbito de projetos específicos que envolvam a produção e publicação de conteúdos com imagem e/ou voz dos alunos, o professor responsável deve obter uma autorização escrita específica por parte do aluno e/ou do encarregado de educação (ver Anexo 3).

c. A autorização para uso de imagem, som ou vídeo dos alunos aplica-se apenas ao ano letivo em curso, devendo ser renovada anualmente no ato de matrícula.

d. A captação de imagens dos alunos para fins de publicação, deve ser feita à distância ou de ângulos que dificultem a identificação, evitando-se também imagens individuais.

e. Os trabalhos dos alunos devem incluir uma ficha técnica, podendo conter uma licença de publicação apropriada, obtida através da plataforma *Creative Commons*.

f. Os professores não estão autorizados a publicar imagens, vídeos ou outros registos de alunos nas suas redes sociais pessoais.

g. Também os alunos e restantes funcionários estão proibidos de publicar, nas suas redes sociais pessoais, imagens recolhidas no interior da Escola que contenham dados pessoais, trabalhos ou imagens de alunos, professores ou funcionários.

h. É expressamente proibida a captação e publicação de fotografias ou vídeos por entidades externas à Escola sem o consentimento informado dos encarregados de educação dos alunos envolvidos. Excetua-se deste ponto a cobertura de eventos públicos como consta no n.º 2 do artigo 79.º do Código Civil.

i. Sempre que solicitado por um encarregado de educação, e caso não haja fundamento legal para manter a publicação, os conteúdos digitais que envolvam o respetivo educando devem ser removidos das plataformas da Escola no prazo razoável.

10.3 Utilização de Redes Sociais e Comunidades Virtuais

a. A Equipa de Transição Digital, em articulação com o Coordenador TIC e/ou o grupo disciplinar de Informática, pode prestar apoio à comunidade escolar através da produção

de conteúdos, sessões de esclarecimento, ações de formação e workshops, consoante disponibilidade e interesse, com vista à promoção de práticas seguras na utilização da Internet.

b. Os professores que pretendam utilizar ferramentas online em contexto curricular devem avaliar previamente os riscos associados aos sítios da Internet, consultando os seus termos e condições, para garantir a adequação às faixas etárias dos alunos.

c. A página web da Escola incluirá uma área dedicada à sensibilização para o uso seguro da Internet, disponibilizando também materiais de apoio dirigidos a pais e encarregados de educação.

d. A utilização de grupos informais em redes sociais ou aplicações de mensagens (ex.: WhatsApp) para comunicação com alunos ou encarregados de educação não é permitida. Toda a comunicação institucional deve ser realizada por canais oficiais da Escola.

e. Os membros da comunidade escolar devem adotar uma conduta ética e responsável nas interações digitais relacionadas com a Escola, mesmo em contextos pessoais.

11 | A Escola reserva-se o direito de:

1. Auditar os serviços de rede e eletrónicos, com o objetivo de verificar o cumprimento das políticas de utilização definidas na presente Política de Utilização Aceitável (PUA).

2. Realizar ações de monitorização e/ou auditoria aos serviços de rede e eletrónicos, por pessoal devidamente autorizado, para efeitos de segurança, diagnóstico e manutenção, garantindo, a confidencialidade da informação dos utilizadores.

3. Analisar denúncias relativas ao incumprimento das normas previstas neste documento. Caso as denúncias se revelem fundamentadas, as entidades envolvidas serão notificadas e deverão proceder, de imediato, à regularização da situação.

4. Solicitar, em situações de risco elevado e para a segurança da infraestrutura ou dos dados, às entidades superiores competentes — nomeadamente à Equipa Infolive da Direção Regional de Informática (DRI) ou à DTSI — o bloqueio imediato e unilateral de contas institucionais, caixas de correio eletrónico, acessos a serviços de rede, pertencentes a pessoas singulares ou coletivas.

5. Reportar à equipa CIBER.EDU, os processos considerados críticos que tenham sido comunicados ao Conselho Executivo, à Equipa de Cibersegurança da Escola.

12 | Responsabilidade

A Escola não se responsabiliza legalmente por qualquer utilização dos serviços, recursos eletrónicos ou da infraestrutura de comunicações que viole a legislação em vigor ou as normas definidas na presente Política de Utilização Aceitável (PUA), recaindo essa responsabilidade exclusivamente sobre os utilizadores.

14 | Conhecimento da PUA

A Escola está comprometida com a segurança digital de toda a comunidade educativa. Para garantir um ambiente offline e online seguro e responsável, implementámos a Política de Utilização Aceitável que será divulgado:

a) ao pessoal docente e não docente:

Através da realização de sessões formativas para explicar as medidas da PUA, boas práticas digitais e procedimentos de segurança. Estas sessões visam capacitar todos os colaboradores para prevenir riscos e proteger dados.

b) aos alunos:

Os alunos serão informados pelo titular/ diretor de turma sobre a existência e importância da PUA, promovendo comportamentos seguros na utilização das tecnologias.

c) aos pais e encarregados de educação:

A Escola comunicará a PUA através de boletins informativos e nas reuniões regulares com os titulares/ diretores de turma, garantindo que todos conhecem as medidas, de forma a apoiar os seus educandos.

Os utilizadores que usufruem dos serviços, recursos eletrónicos e da infraestrutura de comunicações da Escola podem consultar a PUA na página Web da Escola.

- A partir do momento em que lhes são atribuídas as credenciais institucionais de acesso, os utilizadores consideram-se vinculados às normas e princípios definidos na presente PUA.
- O desconhecimento da PUA ou das suas atualizações não isenta o utilizador do cumprimento das regras nela estabelecidas.

- A aceitação da PUA é implícita à utilização dos serviços digitais e plataformas da Escola.
- A violação das regras definidas neste documento implica medidas corretivas ou disciplinares, nos termos da legislação em vigor e do Regulamento Interno da Escola.

Anexo 1 | Estrutura e organização das equipas na Plataforma Teams

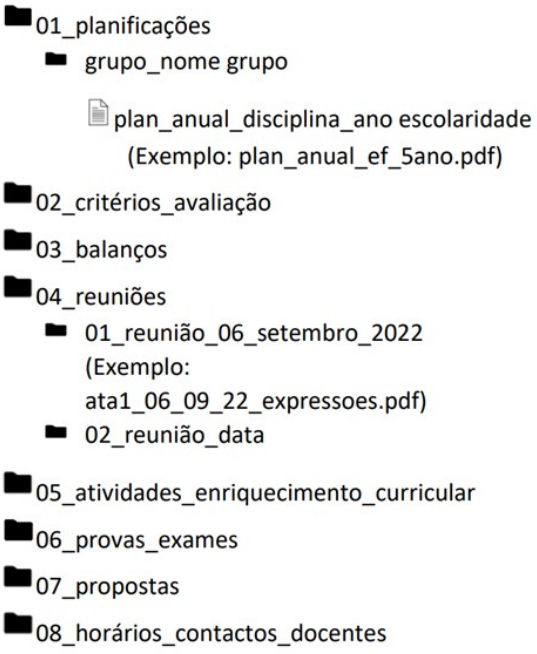
De forma a uniformizar e padronizar um conjunto de procedimentos, em particular a criação e organização das equipas na plataforma Teams, cada docente responsável pela criação de equipas deve seguir as seguintes regras:

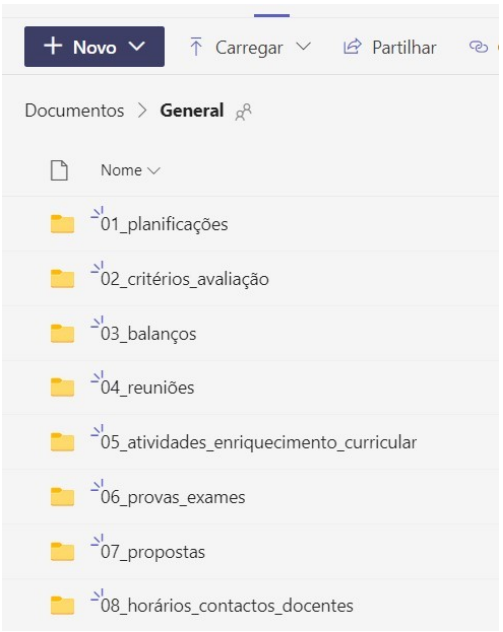
A - Coordenador de Departamento

- 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

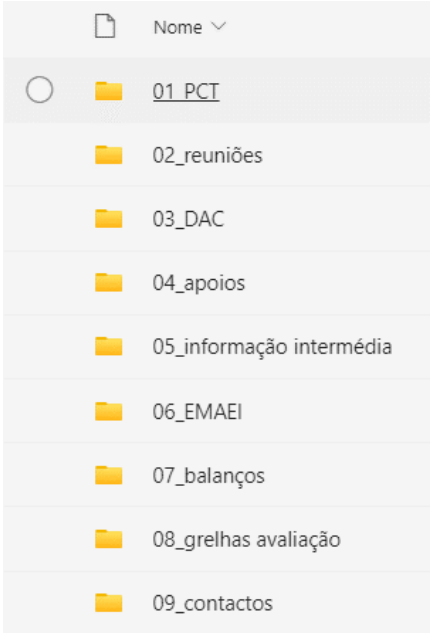
- No final de cada ano letivo, deverá criar uma pasta nomegrupo_anoletivo (matemática2022_2023) e mover todas as pastas para o seu interior.

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.

Anexo 2 | Autorização de captação/ publicação de imagem e trabalhos escolares

S. R.

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
ESCOLA BÁSICA E SECUNDÁRIA/PE DA CALHETA

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 Utilização Aceitável (PUA), para fins exclusivamente de atividades de ensino e divulgação de atividades.

Tomei conhecido da PUA 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 Utilização Aceitável (PUA), para fins exclusivamente de atividades de ensino e divulgação de atividades.

Tomei conhecido da PUA 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)

ESCOLA BÁSICA E SECUNDÁRIA/PE DA CALHETA
Estrada Simão Gonçalves da Câmara nº 39 – 9370-139 Calheta
Tel.: 291 820 000 | ebscalheta@edu.madeira.gov.pt | https://escoladigital.madeira.gov.pt/ebspecalheta/

(formato editável disponível na equipa de pessoal docente na Plataforma Teams)

Anexo 3 | Autorização de recolha de imagem, som e vídeo para projetos e ou atividades

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
ESCOLA BÁSICA E SECUNDÁRIA/PE DA CALHETA

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

Projeto/ Atividade:

Eu, , encarregado de educação do aluno(a) , nº , do anoº , 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 Utilização Aceitável (PUA), 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 / Observações:

Assinatura do Encarregado de Educação

_____

Assinatura do professor:

_____

Tomei conhecimento

___ / ___ / 20 ___

ESCOLA BÁSICA E SECUNDÁRIA/PE DA CALHETA
Estrada Simão Gonçalves da Câmara nº 39 – 9370-139 Calheta
Tel.: 291 820 000 | ebscalheta@edu.madeira.gov.pt | https://escoladigital.madeira.gov.pt/ebspecalheta/

(formato editável disponível na equipa de pessoal docente na Plataforma Teams)