

PUA

POLÍTICA DE UTILIZAÇÃO ACEITÁVEL



David Pinto Teixeira
[Endereço de correio eletrónico]

INTRODUÇÃO

Uma Política de Utilização Aceitável (PUA) é uma ferramenta importante para a gestão de dados e informações nas escolas e outras instituições educacionais. A PUA é um conjunto de regras e diretrizes que definem o que é considerado aceitável em termos de uso dos recursos e dados de uma escola.

A PUA é uma medida de segurança importante que ajuda a proteger a escola e os seus utilizadores contra ameaças cibernéticas e violações de dados. Além disso, ajuda a garantir que os dados pessoais ou sensíveis sejam utilizados de forma adequada e responsável.

A PUA é um documento claro e objetivo e todos os utilizadores da escola devem ser informados da sua existência e conteúdo. Além disso, a PUA deve ser atualizada regularmente para se adequar às mudanças na tecnologia e na legislação.

Mais se refere que o PUA não se assume como uma completa e detalhada política de proteção de dados, vulgo PPD, mas antes como um documento orientador e adaptado à realidade da Escola Secundária de Felgueiras e respeitador do Regulamento Geral de Proteção de Dados (RGPD). Para uma completa PPD deve ser consultado o RI da ESF.

OBJETIVO

Este documento tem como objetivo definir e enquadrar as políticas de utilização responsável dos serviços, recursos eletrónicos, utilização de dados e infraestruturas de comunicação da Escola Secundária de Felgueiras.

ÂMBITO

Este documento visa principalmente a utilização de plataformas digitais e infraestruturas, tais como:

- Plataforma Moodle;
- Google Workspace (Gmail, Google Drive, Classroom, etc.);
- Website da ESF;
- Programa de Gestão de Alunos;
- Programa de Gestão de Funcionários;
- Todas as plataformas/aplicações digitais utilizadas no contexto educacional;
- Equipamentos e redes da Escola Secundária de Felgueiras.

DESTINATÁRIOS

Este documento aplica-se a todos os alunos, professores, Assistentes Operacionais e Assistentes Administrativos, doravante designados por utilizadores.

CONHECIMENTO DA PUA

- Os utilizadores, a partir da atribuição das credenciais institucionais de acesso, passam a estar vinculados à política de utilização aceitável expressa neste documento.
- Os utilizadores são informados, por email, da PUA.
- Este documento está disponível em <https://www.esfelgueiras.pt/>.

POLÍTICAS

1. Propriedade dos dados

- 1.1 É importante compreender que os dados gerados pela escola pertencem a ela, e os utilizadores não têm permissão para copiar, modificar ou apagar esses dados sem autorização;
- 1.2 Os dados gerados pelas escolas incluem informações sobre utilizadores, bem como dados administrativos e financeiros. Esses dados são confidenciais e são protegidos adequadamente para garantir a privacidade de todos os envolvidos;
- 1.3 É importante que os utilizadores, compreendam que os dados são propriedade da escola e não podem ser utilizados de forma inadequada ou prejudicial. É necessário obter permissão antes de copiar, modificar ou apagar esses dados;
- 1.4 Por exemplo, se um professor precisa aceder às informações de um aluno, ele deve fazê-lo de acordo com as políticas de privacidade da escola e apenas para fins educacionais legítimos. Não é permitido ao professor copiar ou modificar essas informações sem autorização prévia.

2. Utilização apropriada

- 2.1 Os utilizadores só podem utilizar os dados para fins educacionais. A utilização dos dados para qualquer outro propósito é proibida. Isto significa que os dados só podem ser utilizados para fins de aprendizagem e investigação, e não podem ser utilizados para fins comerciais, de marketing ou outros fins que não estejam relacionados com o objetivo educacional;
- 2.2 A utilização não autorizada de dados pode levar a violações de privacidade e segurança, bem como a ações legais por parte dos proprietários dos dados;
- 2.3 É punível por lei obter acesso não autorizado a material ou equipamento informático.

3. Passwords

As *passwords* seguras são a primeira linha de defesa para proteger as nossas informações pessoais, financeiras e profissionais online. Por isso, é importante criar *passwords* fortes e seguras e tomar medidas para protegê-las adequadamente.

O utilizador deve adotar as seguintes práticas na criação e gestão de *passwords*:

- 3.1 **Comprimento:** As senhas devem ter pelo menos 12 caracteres. Quanto maior a *password*, mais difícil será para os hackers adivinhá-la;
- 3.2 **Complexidade:** Usar uma mistura de letras maiúsculas e minúsculas, números e símbolos para aumentar a complexidade da *password*;
- 3.3 **Evitar informações pessoais:** Evitar usar informações pessoais como o nome, data de nascimento ou morada, pois essas informações podem ser facilmente descobertas por hackers;
- 3.4 **Usar frases em vez de palavras:** em vez de usar uma palavra comum, usar uma frase aleatória, pois é mais difícil de adivinhar;
- 3.5 **Não reutilizar *password*:** Usar *passwords* exclusivas para cada conta que tem. Isso reduz as hipóteses de que, se uma *password* for comprometida, todas as suas contas sejam comprometidas;
- 3.6 **Usar um gestor de *passwords*:** um gestor de *passwords* é uma ferramenta que pode ajudar a criar e armazenar *passwords* seguras. Ele pode gerar *passwords* aleatórias e armazená-las de forma encriptada, o que dificulta o acesso por parte de hackers;
- 3.7 **Ativar a autenticação de dois fatores:** A autenticação de dois fatores é uma camada adicional de segurança que requer uma segunda forma de autenticação além de uma *password*. Isso pode incluir um código enviado para o seu telefone ou uma impressão digital;
- 3.8 **Mantenha as *passwords* em segurança:** Não partilhar as *passwords* com ninguém. Não as anotar em papel ou enviá-las por e-mail ou mensagem de texto.

4. Política de privacidade

- 4.1 **Obtenção de dados:** A escola deve explicar claramente quais os dados que são recolhidos, as finalidades para as quais são recolhidos e a base de licitude para o tratamento de dados em si, nos termos da legislação em vigor.
- 4.2 **Uso de dados:** Os dados obtidos pelos utilizadores devem ser usados apenas para os fins especificados. Devem garantir que os dados não sejam partilhados com terceiros sem consentimento explícito dos titulares dos dados;
- 4.3 **Proteção de dados:** Devem ser adotadas medidas razoáveis para proteger os dados pessoais que se recolhem, utilizam e armazenam. Isso pode incluir o uso de *passwords* seguras, criptografia de dados e sistemas de segurança de rede;
- 4.4 **Retenção de dados:** Os dados pessoais devem ser conservados apenas pelo tempo necessário para atingir os fins para os quais foram obtidos. Após esse período, os dados devem ser eliminados ou anonimizados;
- 4.5 **Direitos dos titulares dos dados:** Deve-se garantir que os titulares dos dados tenham direito a aceder, corrigir ou solicitar a eliminação dos seus dados pessoais. De igual modo, os titulares devem poder opor-se ao tratamento dos seus dados pessoais e a decisões automatizadas tomadas sobre si com base nos seus dados pessoais, bem como a solicitar a limitação do tratamento dos seus dados. Nessa senda, os titulares devem ser informados relativamente aos contactos junto dos quais poderão exercer os seus direitos de proteção de dados ou solicitar os seus devidos esclarecimentos. Além disso, os titulares dos dados devem ser informados sobre quaisquer violações de dados que possam afetar a sua privacidade
- 4.6 **Dever de informação:** A escola deve informar os titulares relativamente às informações mencionadas nos pontos anteriores, sob a forma de políticas de proteção de dados de fácil acesso e consulta. De igual modo, cada política deve elencar os possíveis destinatários para os quais os dados possam ser enviados, bem como eventuais países terceiros para os quais se possam transferir os dados. Nestas políticas, os titulares devem ser informados quanto à sua capacidade de apresentarem reclamação para a Comissão Nacional de Proteção de Dados caso estejam insatisfeitos com a resposta dada ao seu pedido de exercício de direitos.
- 4.7 **Formação de utilizadores:** A escola deve fornecer informação regular aos seus utilizadores sobre as políticas de privacidade de dados e a importância de proteger os dados pessoais dos titulares dos dados;

5. Monitorização

Para garantir o cumprimento regras expostas neste documento, a escola pode adotar as seguintes medidas de monitorização:

- 5.1 **Monitorização de rede:** A escola pode monitorizar a rede de computadores para detetar atividades suspeitas ou violações da política de utilização aceitável. Isso pode incluir a monitorização de tráfego de rede, *logs* de servidor, análise de malware, entre outros;

- 5.2 **Auditorias regulares:** A escola pode realizar auditorias regulares das contas de utilizadores para identificar atividades não autorizadas ou violações da política de utilização aceitável. Isso pode incluir a revisão de registos de acesso, *logs* de segurança e históricos de atividade;
- 5.3 **Restrições de acesso:** A escola pode restringir o acesso a determinados recursos ou sites da internet, como redes sociais ou sites de jogos, que possam ser considerados inapropriados ou que possam comprometer a segurança da rede;
- 5.4 **Políticas de *password*:** A escola pode implementar políticas de senha para garantir que os utilizadores escolham *passwords* seguras e as mudem regularmente;
- 5.5 **Conscientização dos utilizadores:** A escola pode realizar ações de sensibilização regulares para conscientizar os utilizadores sobre a política de utilização aceitável e os riscos associados ao uso inadequado dos recursos das tecnologias da informação.

6. Violações

Caso algum utilizador viole a PUA a escola pode aplicar sanções disciplinares para garantir que as regras sejam respeitadas e para manter os utilizadores num ambiente de aprendizagem seguro e produtivo. Algumas sanções que podem ser aplicadas incluem:

- 6.1 **Advertência verbal ou escrita:** Uma advertência verbal ou escrita é uma forma leve de sanção que pode ser aplicada a um utilizador que comete uma infração menor ou pela primeira vez. Ela tem como objetivo alertar o utilizador sobre a violação da política e incentivá-lo a cumprir as regras;
- 6.2 **Suspensão do acesso:** Em casos mais graves, a escola pode suspender temporariamente o acesso do utilizador aos recursos das tecnologias de informação. Isso pode ser feito para evitar que o utilizador continue a violar a política e para proteger a segurança da rede;
- 6.3 **Restrições de acesso:** Em alguns casos, a escola pode restringir o acesso do utilizador a determinados recursos ou serviços, como sites da internet ou redes sociais, que possam estar relacionados com a violação da política;
- 6.4 **Sanções disciplinares:** A escola pode adotar medidas disciplinares, como advertências, suspensões ou expulsões, para os utilizadores que violem a política de utilização aceitável.

7. Atualizações

- 7.1 PUA é revista e atualizada regularmente para garantir que esteja alinhada com as práticas e regulamentações atuais;
- 7.2 As alterações são comunicadas por e-mail a toda a comunidade educativa e constam também na página web da Escola Secundária de Felgueiras em <https://www.esfelgueiras.pt/>.

8. Regulamento Geral sobre a Proteção de Dados (RGPD)

- 8.1 Este documento foi elaborado em conformidade com as normas e regulamentos em vigor, incluindo o RGPD e a sua lei de execução no ordenamento jurídico português, para garantir que a proteção de dados pessoais seja mantida.
- 8.2 Qualquer situação omissa neste documento, deve-se aplicar as normas constantes no RGPD e na sua respetiva lei de execução no ordenamento jurídico português.

9. Outras Políticas

- 9.1 Não instalar qualquer software adquirido ou descarregado, sem permissão do responsável pelo sistema ou da direção da escola;
- 9.2 Não guardar documentos que contenham informações pessoais ou sensíveis, fotografias, etc., nos computadores de utilização comum da escola;
- 9.3 Respeitar sempre os direitos de autor e propriedade intelectual referenciando sempre a origem da informação;
- 9.4 As comunicações eletrónicas com os alunos e pais/encarregados de educação são realizadas exclusivamente através de canais de comunicação aprovados pela direção da escola;
- 9.5 É proibido criar, transmitir, apresentar, publicar ou encaminhar qualquer tipo de material suscetível de assediar e ofender cidadãos;
- 9.6 Em caso de detetar um comprometimento/violação de dados, o utilizador deve comunicar imediatamente o sucedido à direção da escola para que esta tome as medidas necessárias para a resolução do problema;
- 9.7 As credenciais de acesso às plataformas atribuídas pela escola são da responsabilidade do utilizador, pelo que, este deve adotar as medidas aqui descritas para as manter em segurança;
- 9.8 Terminar sempre as sessões nos computadores de utilização comum da escola. Neste caso, o aluno deve abrir sempre o navegador no modo “anónimo” para que as suas sessões nunca fiquem ativas depois de fechar a janela de navegação.

CONCLUSÃO

A Política de Utilização Aceitável é uma ferramenta importante para garantir que os dados sejam utilizados de forma ética e responsável. É um conjunto de regras estabelecidas pela escola para regulamentar o uso de seus recursos de computação, comunicação e utilização de dados.

A PUA inclui diretrizes sobre o uso apropriado da Internet, e-mail, redes sociais e outros recursos tecnológicos, e define as consequências para violações das políticas.

A PUA é projetada para garantir que os utilizadores dos recursos tecnológicos da escola respeitem as leis aplicáveis, as normas éticas e os interesses da escola, bem como a privacidade e segurança dos dados dos utilizadores.