POLÍTICA DE UTILIZAÇÃO ACEITÁVEL (PUA)

DAS INFRAESTRUTURAS TECNOLÓGICAS

E DE SERVIÇOS DE TIC

Aprovada pelo Conselho Pedagógico

a 04 de novembro de 2020

A *Política de Utilização Aceitável* (*PUA*) *das infraestruturas tecnológicas e de serviços de TIC* da Escola Secundária de Avelar Brotero (ESAB), doravante designada simplesmente *PUA*, complementa-se com a *Política de Segurança Digital* e com a *Política de Privacidade e de Proteção de Dados Pessoais*, em conformidade com o *Regulamento Geral de Proteção de Dados* (*RGPD*: *Regulamento 2016/679* do Parlamento Europeu e do Conselho de 27 de abril de 2016) e com a *Lei* 58/2019 de 8 de agosto, e cumpre as exigências legalmente prescritas pelos artigos 136.º, n.º 1, e 136.º, n.º 4 do *Código de Procedimento Administrativo* (aprovado pelo Decreto-Lei n.º 4/2015, de 07 de Janeiro), tendo em vista a aplicação efetiva do *RGPD* no quadro das características da Escola, uma conduta digital ética e legal da comunidade escolar e a proteção dos sistemas e serviços para segurança de todos.

A garantia do respeito das regras que sustentam a *PUA* possibilita o correto funcionamento dos dispositivos e serviços digitais na e da Escola.

As linhas de conduta da *PUA* constituem direitos e deveres dos utilizadores das redes e dos sistemas informáticos da ESAB.

1. Objeto, âmbito de aplicação e utilizadores

A *PUA* tem como objetivo estabelecer os princípios orientadores da utilização adequada dos sistemas informáticos e redes de telecomunicações da Escola, salvaguardando o seu desígnio educativo, a sua reputação institucional e a segurança digital da organização e dos seus utilizadores.

A *PUA* é aplicável a docentes, discentes ou alunos, assistentes operacionais, assistentes técnicos, encarregados de educação, convidados e a todos os que utilizam recursos digitais, equipamentos, redes e serviços de TIC da instituição ou na instituição.

2. Princípios de uso ético das infraestruturas tecnológicas e restrições

Na utilização das infraestruturas tecnológicas da Escola, aplica-se o *princípio da responsabilidade*, que implica a não aceitação de comportamentos que interfiram ou possam interferir, de forma lesiva, outros utilizadores ou serviços, sejam eles internos ou externos à Escola, nomeadamente com o propósito do exercício de atividades ilegais ou ilegítimas, do desrespeito da integridade física e moral dos membros da comunidade escolar e de outros (tais como atos ofensivos ou discriminatórios por motivos de religião, sexo, ou género, atos de assédio sexual, pedofilia, de *bullying*, *cyberbullying*, racismo, xenofobia, terrorismo, difamação, *fishing*, etc.), da criação, da transmissão ou do acesso a conteúdos sem respeito pelos direitos de propriedade intelectual, de autor e conexos, de acesso não autorizado a sistemas ou infraestruturas tecnológicas da Escola que vulnerabilize a sua segurança.

A Escola reserva-se o direito aplicar medidas de contenção nas situações em que entender que a utilização dos seus recursos tecnológicos não está de acordo com a sua *PUA*.

Assim sendo, assume-se que nenhum recurso tecnológico da Escola pode ser usado:

- para fins não éticos ou ilegais por natureza, ou que violem o espírito de leis locais ou internacionais;

- para fins que entrem em conflito com a missão educativa ou políticas da ESAB, tais como a promoção de causas de política partidária ou a transferência ou armazenamento de material que contenha referências obscenas ou pornográficas, propaganda terrorista e discurso de ódio;
- para fins comerciais, pondo em causa o nome, a reputação e a missão educativa da Escola;
- para fins pessoais ou de terceiros, sem a permissão do Diretor;
- para obstrução do trabalho de terceiros danificando equipamento deliberadamente ou consumindo quantidades exageradas dos recursos do sistema;
- para aceder a computadores ou sistemas confidenciais da Escola;
- para usar os mecanismos de acesso atribuídos a outra pessoa, sem o seu consentimento e assunção de responsabilidade;
- para partilhar ou emprestar contas ou senhas/ palavras-passe de outros, violando o sigilo das contas e pondo em causa a sua segurança digital;
- para copiar *software* e recursos digitais da ESAB sem autorização superior, tendo em vista a partilha, a cedência, ou a venda; e
- para fins que atentem contra a segurança, a privacidade e a proteção de dados pessoais, e que se enquadrem no âmbito da criminalidade informática.

Espera-se que as condutas dos utilizadores estejam de acordo com as leis aplicáveis e com o disposto nesta *PUA*, sendo que a ignorância delas não serve de justificação para a sua violação.

Qualquer utilização não autorizada dos recursos disponibilizados pelas infraestruturas tecnológicas da Escola é considerada indevida e, como tal, passível de procedimento disciplinar e, eventualmente, também criminal.

3. Identificação e autorização de utilizadores

Com exceção dos conteúdos disponibilizados publicamente, o acesso aos recursos digitais da ESAB é efetuado mediante a atribuição de *credenciais de acesso* específicas.

O princípio base de criação de *contas de utilizadores* para acesso às infraestruturas tecnológicas da ESAB atende ao perfil do utilizador, bem como ao recurso e/ou serviço que o mesmo necessita de aceder. Tendo também em consideração que a ESAB como fornecedora de Identidade tem como responsabilidade o fornecimento de asserções de identidade confiáveis e exatas a serviços próprios e de terceiros, torna-se essencial garantir um processo de atribuição de credenciais com elevado grau de confiabilidade e segurança, obrigando a uma maior responsabilização dos intervenientes em todo o processo.

A ESAB no processo de atribuição de identidade a utilizadores recolhe no mínimo os dados: nome, email e número de identificação do titular. As contas associadas a um utilizador são sempre acompanhadas de uma data de expiração adequada ao seu perfil, ao motivo de criação (o direito de acesso) e ao *terminus* do vínculo.

As contas de utilizadores são criadas pelo responsável das infraestruturas tecnológicas da ESAB (administrador) no âmbito das suas atribuições.

As autorizações atribuídas são pessoais e intransmissíveis, competindo ao utilizador manter a confidencialidade e a proteção das credenciais fornecidas.

Para proteger a integridade dos sistemas informáticos ou para observar utilizadores suspeitos de uso não autorizado, o administrador da ESAB pode, quando necessário, suspender ou remover o acesso à rede ou computadores da Escola.

Todo o utilizador que encontrar uma possível quebra de segurança em qualquer sistema informático da Escola deve relatá-la ao Diretor. Não deve tentar usar o sistema sob estas circunstâncias até que o administrador do sistema investigue o problema.

Todo o utilizador ciente do uso não ético ou proibido de recursos informáticos da ESAB deve informar de imediato o Diretor.

Não é ética a conduta frívola, imprópria ou perturbadora no uso dos recursos digitais da Escola.

As violações das regras estabelecidas podem conduzir à suspensão da(s) conta(s) de utilizador, sem compromisso de eventual aplicação de procedimento disciplinar e/ou criminal.

4. Segurança de sistemas e redes

Não é permitido aos utilizadores a violação ou tentativa de violação dos sistemas, em especial do sistema de segurança, e das redes da infraestrutura tecnológica da ESAB.

Assim, não são permitidas as seguintes ações:

- disseminação intencional de *vírus*, *Trojans*, *Malware* ou qualquer outro *software* prejudicial ou nocivo aos utilizadores da *Internet*;
- utilização de *Software* desatualizado ou com falhas conhecidas, que possibilitem a sua exploração para tomar controlo do servidor, ou de *Software* sem o devido licenciamento;
- partilha e/ou troca de *Software* ou informação protegida por direitos de autor;
- recurso a *Software* que permita o uso dos servidores como *Open Relay* ou *Open Proxy*;
- instalação de *Proxies* ou NAT;
- instalação de anonimizadores;
- entrada ou tentativa de entrada em servidores sem autorização;
- uso de *cracking*, *brute-force* ou ataques de dicionário para acessos não autorizados;
- deteção automática de serviços em servidores (*Port scan*);
- pesquisa não autorizada de vulnerabilidades em servidores, serviços e redes;
- interferência intencional no bom funcionamento de servidores, serviços ou redes (ação de sobrecarga dos serviços - *Denial of service*, envio em massa de pacotes - *Flooding* e tentativas de bloqueio ou perturbação de serviço, servidores ou redes); e
- falsificação de dados com a intenção de ludibriar e induzir em erro os recetores de dados (alterações de endereços IP - *IP Spoofing*, alterações de endereços ARP - *ARP Spoofing* e alterações dos cabeçalhos das mensagens de correio eletrónico).

5. Uso de sistemas informáticos administrativos

Os sistemas administrativos da ESAB contêm dados escolares, financeiros e pessoais sensíveis e confidenciais. O acesso a esses sistemas é limitado unicamente a utilizadores explicitamente autorizados. Este privilégio é uma confiança e uma responsabilidade. O emprego errado do privilégio de acesso ou o acesso não autorizado aos sistemas é uma violação desta *PUA*.

Todo o utilizador (professor, assistente técnico, assistente operacional, estudante, ou encarregado de educação) da ESAB que tenha conhecimento de uma violação desta *PUA* deve relatá-la ao Diretor e/ou fazer o registo do incidente pelo método estabelecido para o efeito pela Escola. A falha em relatar tal conhecimento é uma ocultação ou negligência grave, passível de procedimento disciplinar.

Todos os utilizadores digitais da ESAB que intencionalmente acedam ou facultem o acesso aos sistemas e às redes informáticas, que alterem, falseiem, adicionem, suprimam, danifiquem ou destruam dados neles contidos serão sujeitos a processo disciplinar e criminal se tal se justificar.

6. Correio eletrónico (*e-mail*) e política *anti-SPAM*

O uso abusivo do correio eletrónico causa transtornos e prejuízos à infraestrutura da ESAB, assim como aos seus utilizadores, ao afetar o normal funcionamento dos sistemas e dos serviços digitais.

O ecossistema da *Google Suite for Education* da ESAB barra sistemicamente qualquer tipo de SPAM (acrónimo da locução inglesa *Sending and Posting Advertisement in Mass* 'enviar e alocar publicidade em massa' com intuito comercial e não solicitada pelo destinatário), evitando assim qualquer mensagem por *e-mail* que possa causar impacto negativo nos utilizadores e nas infraestruturas tecnológicas da Escola ou colocar endereços IP dos utentes de correio eletrónico em listas negras.

Assim, também não é permitido:

- o envio de SPAM ou *SPAM traps*;
- o envio de mensagens por *e-mail* a quem tenha solicitado o seu cancelamento;
- o envio massivo de mensagens por *e-mail* não autorizadas (*SPAMMING*);
- o envio de mensagens em cadeia (*chain letters*) ou outras mensagens de incómodo ou assédio;
- o uso dos servidores como SMTP "*Open Proxy*" ou "*Open Relay*".

7.Intervenção do administrador das infraestruturas tecnológicas

Sempre que o administrador das infraestruturas tecnológicas da ESAB detete ou tenha conhecimento de atos abusivos nos seus servidores ou nas redes e for necessária a sua intervenção para os resolver, pode, sem qualquer consulta do(s) utilizador(es) prevaricador(es), optar por:

a) avisar o infrator por *e-mail*, telefone ou pessoalmente, concedendo-lhe um prazo muito restrito para parar com o abuso ou a violação da atual *PUA*;
b) efetuar a necessária intervenção para resolução imediata do problema, sendo o infrator sujeito a um processo disciplinar e à eventual indemnização de danos causados;
c) suspender/ cancelar de imediato o serviço, sem aviso prévio, caso a gravidade da situação o justifique, com consequências disciplinares.

8. Monitorização do uso da *Internet* de acordo com a Política de Privacidade e de Proteção de dados pessoais

No cumprimento das suas obrigações institucionais e legais, nomeadamente das decorrentes da *Política de Privacidade e de Segurança de Dados Pessoais* a ESAB monitoriza e regista a utilização das infraestruturas tecnológicas sob sua gestão, com o objetivo de conservar os registos considerados necessários para o correto suporte técnico dos equipamentos e garantir segurança das infraestruturas.

Tal monitorização é realizada em consonância com os requisitos mínimos das redes e sistemas de informação preceituados na *Resolução de Conselho de Ministros 41/2018*, no estrito cumprimento do interesse da organização e dos seus utilizadores.

A ESAB garante, assim, a não interferência nas comunicações eletrónicas protegidas por algoritmos criptográficos, respeitando os direitos, bem como a privacidade e liberdade dos seus utilizadores.

A monitorização recolhe dados referentes à utilização das infraestruturas de forma pseudonimizada, compreendendo apenas os dados necessários para os efeitos previamente identificados, nomeadamente endereço IP, endereço MAC, impressão digital do navegador, *browser* ou navegador de *Internet* utilizado e sistema operativo pelo *browser's user agent string*, portas dos protocolos TCP e UDP, data, hora, metadados relativos às camadas 3 (rede) e 4 (transporte) do modelo *Open System Interconnection* (OSI), ligações de saída e termos de pesquisa.

Na ausência de outro prazo de conservação definido nas condições de utilização próprias do serviço ou por imposição legal, os registos serão mantidos por um período máximo de 24 meses.

É expressamente proibido o acesso a estes registos a qualquer pessoa, além do administrador.

O acesso pelo administrador apenas é autorizado no âmbito do processo de monitorização de segurança das infraestruturas ou em situações excecionais e justificadas para despistes técnicos ou cumprimento de obrigações legais.

9.Responsabilidade de abusos, usos indevidos, ilícitos ou criminosos

A ESAB não assume qualquer responsabilidade institucional por abusos, usos indevidos, ilícitos ou criminosos das suas infraestruturas tecnológicas.

Tais práticas são da inteira responsabilidade do(s) seu(s) autor(es) e atentam contra a *PUA*, a *Política de Segurança Digital*, a *Política de Privacidade e de Proteção de Dados Pessoais*, o *Projeto Educativo* e o *Regulamento Interno* da Escola.

Poderão, por isso, ser alvo de procedimento disciplinar instaurado pelo Diretor, de *notificação* ao *Centro Nacional de Cibersegurança* (nomeadamente os *incidentes* de *malware*; de *disponibilidade*[1]; de *recolha de informação* acerca do sistema informático e/ou das redes, de monitorização e leitura não autorizada de tráfego de rede, ou acerca dos utilizadores ou do sistema através de métodos de

[1] *Disponibilidade*: disrupção da capacidade de processamento e resposta dos sistemas e redes de forma a torná-los inoperacionais, ou ação premeditada para danificar um sistema, interromper um processo, alterar ou eliminar informação, etc..

phishing; de *intrusão* ou *tentativa de intrusão*[2]; de *quebra da segurança de informação*[3]; de *fraude*[4]; de *conteúdo abusivo*[5]; ou de outra natureza), tal como no caso de *violação de dados pessoais* de *notificação* ao *Centro Nacional de Proteção de Dados* (nos termos do artigo 33.º do *RGPD*), e, em *casos* de *ilícito criminal* ou *cibercriminalidade*, de *comunicação* à *Polícia Judiciária*, ou ao órgão de polícia criminal competente cujo procedimento penal dependa de queixa ou de acusação particular.

10. Atualização ou alterações da *PUA*

A ESAB reserva-se o direito de, a qualquer momento, proceder a atualizações ou alterações da *Política de Utilização Aceitável* e de as divulgar em espaço próprio para o efeito.

Coimbra, 04 de novembro de 2020

O Diretor

_____

[2] *Intrusão* para exploração de uma vulnerabilidade no sistema, numa componente ou na rede, ou para fazer *login* em serviços ou mecanismos de autenticação/controlo de acesso.
[3] *Quebra da segurança de informação*: por exemplo, para acesso não autorizado a um determinado conjunto de informações, ou para a sua alteração ou eliminação não autorizada.
[4] *Fraude*: por exemplo, utilização de recursos da instituição para fins diferentes ou de utilização de nome da instituição sem autorização.
[5] *Conteúdo abusivo*: por exemplo, envio de mensagens de SPAM, de distribuição ou partilha de conteúdos protegidos por direitos de autor, ou de disseminação de conteúdos proibidos por lei.