Manual de procedimentos
Sistemas informáticos

Agrupamento de Escolas de Fornos de Algodres
dezembro 2017
www.ae-fa.pt
direcao@ae-fa.pt

Índice

Glossário

AEFA – Agrupamento de Escolas de Fornos de Algodres

GARE – Gestor de Atividades e Recursos Educativos

GIAE – Gestão Integrada para Administração Escolar

PTE – Plano Tecnológico da Educação

SAE – Serviços de Administração Escolar

MEC – Ministério da Educação e Ciência

Vírus informáticos - são programas de computador que se inserem em ficheiros. Estes, ao serem utilizados, provocam danos em outros ficheiros e mesmo nos computadores, apagando ou alterando dados e tornando as máquinas inoperativas.

Troianos - são tipos específicos de vírus informáticos que se disfarçam, aparecendo como programas que executam determinadas tarefas úteis.

Worms ("vermes") são outro tipo de vírus, que se propagam através dos computadores, criando várias cópias em cada um deles e provocando a sua paragem.

Malware – que tem o significado de "software maldoso" ou "malicioso" – designa um conjunto enorme de programas criados e distribuídos com o intuito de alterar dados, roubar informação ou danificar fisicamente os computadores.

Spam - designa o email não solicitado que é enviado para o maior número de destinos possível com objetivos comerciais ou com conteúdos não apropriados ou com temas irrelevantes e sem interesse para o destinatário.

Phishing - é uma forma fraudulenta de adquirir dados confidenciais, tais como: palavras-passe e códigos de contas bancárias e cartões de crédito. Num email – aparentemente de fonte fidedigna – o utilizador, ao clicar num link, é levado a uma página em tudo idêntica à do seu banco, onde, a pretexto de uma falsa confirmação de dados, é convidado a introduzir os seus códigos de acesso. Ao fazê-lo, sem se dar conta disso, o utilizador fornece os seus dados a outros que os irão utilizar para seu proveito. Só no ano de 2007, nos Estados Unidos, foram perdidos para esta atividade criminosa cerca de 3,2 biliões de dólares.

Hacker - é alguém que utiliza os seus conhecimentos informáticos para fins ilegais, introduzindo-se nos sistemas com o objetivo de alterar ou roubar dados, seja para proveito pessoal, seja para defesa de uma causa social ou política.

Firewall - é um programa informático que monitoriza, em permanência, as ligações do nosso computador com o exterior, especialmente com a Internet, evitando intromissões indesejadas no nosso sistema.

Introdução

O presente documento foi elaborado com o objetivo de informar os utilizadores dos recursos informáticos e computacionais acerca das normas e procedimentos que regem a utilização destes na Escola Básica e Secundária de Fornos de Algodres, bem como os procedimentos de solicitação de serviços. As normas e procedimentos foram baseados nas diretrizes legais vigentes e visam a utilização racional e consciente destes recursos e serviços, bem como a preservação e integridade de dados e utilizadores.

Na elaboração deste documento participou a equipa de Manutenção e Gestão de Recursos Tecnológicos (MGRT) e a direção do AEFA.

Recursos do AEFA

Responsáveis por recursos informáticos

Nome	Serviço /Função	Programas/Recurso	Função
Marco Fernandes	Direção/ Adjunto	Gestão de utilizadores da rede do AEFA	Gestão de utilizadores na EdgeBox do AEFA
		Moodle do AEFA	Administração/configuração
		GARE do AEFA	Administração/configuração
		Impressora da sala de professores	Gestão de utilizadores
		Programas Exames	Gestão e utilizador
		Office 365 do AEFA	Administração/configuração
		JPM - software	Administração/gestão de utilizadores
Horácio Carreira	Direção/ Subdiretor	Página do AEFA	Gestão de utilizadores e de conteúdos
Vítor Silva	Docente	Programas Exames	Gestão e utilizador
Pedro Freitas	Bibliotecário	Bibliobase	Gestão e utilizador
Otília Pina	SAE/Coordena-dora Técnica	JPM - software	Administração/gestão de utilizadores
		Programas Exames	Gestão e utilizador
Maria João Santos	SAE/Assistente técnica	JPM - software	Administração/gestão de utilizadores
Em função da designação anual da equipa MGRT		Computadores e equipamentos informáticos	Gestão do parque informático – hardware e software

Equipamentos disponíveis

Em todas as salas de aula existe pelo menos um computador e um projetor para uso pedagógico. Nesses computadores são criadas três contas de utilizador, a saber: “AEFA”, “PTE” e “Master”, todas com recurso a password.

Nas salas de trabalho, para docentes, há pelo menos um computador com três contas de utilizador, a saber: “AEFA”, “PTE” e “Master”, as duas últimas com recurso a password.

Nas salas com computadores destinados a alunos, são apresentadas três contas de utilizador, a saber: “Aluno”, “PTE” e “Master”, as duas últimas com recurso a password.

Todos os computadores da escola sede terão obrigatoriamente uma conta de administrador, designada por “PTE” e uma conta de utilizador sem privilégios de administração.

O objetivo das contas de utilizador é tentar evitar a instalação de software nocivo e alterações nas configurações dos computadores.

Existem cinco quiosques em funcionamento na escola, onde se pode adquirir senhas para almoço e para o bar, consultar saldos e extratos.

A instalação de software e alteração de configurações terá que ser solicitada à direção do AEFA que fará chegar esse pedido à equipa MGRT.

Utilização de dispositivos amovíveis

Os dispositivos de armazenamento amovíveis são todo o tipo de meios que podem ser lidos e/ou gravados pelo utilizador final e que podem ser ligados e desligados a qualquer computador sem que este tenha de sofrer qualquer tipo de modificação. Entre os vários tipos de dispositivos, contam-se os dispositivos de memória flash, como câmaras, leitores de MP3, discos externos, CD e DVD e pens USB. A utilização de dispositivos de armazenamento de dados amovíveis constitui uma fonte bem conhecida de infeções por malware e está diretamente ligada à perda de informações confidenciais de muitas instituições. É essencial adotar medidas adequadas a fim de minimizar o risco de perda ou divulgação de informações confidenciais e reduzir o risco de infeções por malware nos computadores das escolas.

Assim, estabelecem-se as seguintes orientações:

- Não é permitido o uso destes dispositivos nos computadores dos SAE, excetuam-se os dispositivos do próprio serviço;
- Todos os professores e alunos devem analisar os dispositivos amovíveis antes de os usarem com o intuito de detetarem eventual malware, recorrendo ao antivírus do PC;
- É autorizada a utilização de dispositivos amovíveis quando estritamente necessário para fins de ensino/aprendizagem;
- Alunos e professores não estão autorizados, por exemplo, a ligar a sua máquina fotográfica, telemóvel ou leitor MP3 a um computador da escola, exceto se necessitarem de o fazer no âmbito de determinada tarefa que lhes tenha sido atribuída;
- Os docentes devem usar os recursos para armazenamento disponibilizados pelo AEFA, nomeadamente a Onedrive do AEFA – Office 365;
- Os professores devem evitar guardar dados confidenciais dos alunos e de outros elementos da escola nestes dispositivos, exceto se necessário para a execução de tarefas que lhes sejam atribuídas, uma vez que existe sempre o risco de estes dispositivos serem roubados ou perdidos com os dados pessoais gravados.

Internet no AEFA

Todos os alunos e funcionários do AEFA têm acesso à rede sem fios com credencias pessoais e intransmissíveis.

A utilização da Internet é uma ferramenta essencial na aprendizagem, e tem como objetivo elevar os padrões educativos, promover o sucesso dos alunos, apoiar o trabalho dos professores e reforçar a administração escolar.

O acesso à Internet é um direito dos alunos que demonstrem responsabilidade e maturidade na sua utilização, no entanto o acesso dos utilizadores ou computadores à rede podem ser restringidos ou mesmo barrados, se for detetada uma utilização que possa pôr em causa a segurança ou bom funcionamento da rede.

Assim, estabelecem-se as seguintes orientações:

- Os utilizadores devem agir com razoabilidade — por exemplo, descarregar ficheiros de grande dimensão durante o horário de trabalho afeta a qualidade/velocidade da ligação à Internet das restantes pessoas;
- Os utilizadores devem assumir responsabilidade pela sua utilização da Internet;
- Os computadores de trabalho estão protegidos contra determinadas ações inadvertidas ou deliberadas dos utilizadores, pelo que haverá situações em que os utilizadores não conseguirão aceder a páginas e determinados ficheiros;
- Toda a rede tem instalada e atualizada uma proteção antivírus e firewall;
- São criadas redes virtuais diferentes de acordo com a utilização, a saber professor, aluno, administrativo e convidado;
- O acesso por dispositivos sem fios é administrado proactivamente e está sujeito a um nível de segurança com encriptação WPA2.

Aplicações em funcionamento no AEFA

Os dados confidenciais de uma escola incluem, entre outros, dados pessoais de alunos, pais, corpo docente e corpo não docente, registos académicos, médicos e psicológicos dos alunos, dados relativos aos salários e carreiras profissionais dos elementos da escola, bem como dados relativos à própria gestão da escola. Estes dados são guardados nos computadores locais, em dispositivos amovíveis de armazenamento, servidores localizados na escola ou noutro local e em impressões. A proteção insuficiente ou a divulgação inadequada deste tipo de dados pode resultar numa violação da privacidade ou na violação das leis de proteção de dados.

Assim, estabelecem-se as seguintes orientações:

- São criadas redes virtuais diferentes de acordo com a utilização, a saber professor, aluno, administrativo e convidado;
- Não é permitido copiar dados confidenciais dos sistemas administrativos;
- Não deixar documentos confidenciais abandonados em impressoras de acesso público;
- Destruir os documentos com informação confidencial em detrimento de os colocar no caixote do lixo/papelão;
- Evitar recolher dados confidenciais, exceto quando necessário.

Aplicações dos SAE

As aplicações em uso no SAE são, na maioria, disponibilizados pela JPM Abreu, a saber Multiusos, Alunos, SASE, GIAE (Sumários, Portaria, POS) Contab, CIBE, GPV e Oficiar. Há também programas fornecidos pelo MEC, tais como o PFEB, ENEB e ENES, entre outros necessários ao bom funcionamento dos serviços.

Também são utilizadas diversas plataformas e páginas de internet onde se comunicam diversas informações e que devem ser utilizadas com extremo cuidado e com segurança.

Atendendo à diversidade de meios utilizados é importante definir regras de utilização e de segurança.

Assim, estabelecem-se as seguintes orientações:

- Os acessos às diversas aplicações deve ser realizado com recurso à utilização de utilizador/password pessoal;
- As permissões dadas a cada utilizador são as mínimas necessárias para a execução das suas funções, isto é, são adequadas ao posto de trabalho em causa;
- A responsável pela atribuição de permissões no âmbito das aplicações e programas usados no SAE é a Coordenadora Técnica, que será coadjuvada nessas funções por uma assistente técnica;
- As assistentes técnicas não deverão fornecer dados confidenciais aos utentes do serviço sem autorização prévia da direção;
- Diariamente deverá ser feita uma cópia de segurança manual dos programas da JPM, de acordo com um calendário afixado no SAE;

Registo de Imagem

Fotografias e registos vídeo e áudio emprestam dinamismo e interesse a uma publicação, especialmente se incluírem alunos. No entanto, a segurança de alunos e restantes elementos da escola é primordial. Embora frequente nos jornais, a publicação de nomes e fotografias de alunos não é aceitável. Imagens publicadas no passado podem ser reutilizadas, em particular se se tratar de imagens de alunos individuais.

As estratégias a seguir passam por usar imagens relativamente pequenas de grupos de alunos ou imagens que não mostrem rostos visíveis. As fotografias tiradas “de lado” podem substituir as fotografias "de frente" sem se perder a mensagem sobre a atividade pedagógica em questão. As fotografias pessoais podem ser substituídas por autorretratos ou imagens do trabalho dos alunos ou de uma atividade de grupo.

Não devem ser publicadas fotografias de alunos sem autorização prévia por escrito dos pais ou encarregados de educação.

Assim, estabelecem-se as seguintes orientações:

- Os nomes completos dos alunos não serão utilizados em parte alguma do *site* da escola, em especial junto a fotografias;
- Antes da publicação de qualquer imagem/vídeo de alunos, será obtida autorização por escrito dos pais ou encarregados de educação;
- De acordo com o regulamento interno, nos deveres do aluno:
    - não captar sons ou imagens, designadamente, de atividades letivas e não letivas, sem autorização prévia dos professores, dos responsáveis pela direção da escola ou supervisão dos trabalhos ou atividades em curso, bem como, quando for o caso, de qualquer membro da comunidade escolar ou educativa cuja imagem possa, ainda que involuntariamente, ficar registada;
    - não difundir, na escola ou fora dela, nomeadamente, via internet ou através de outros meios de comunicação, sons ou imagens captados nos momentos letivos e não letivos, sem autorização do diretor do AEFA;

Bibliografia

http://www.esafetylabel.eu (07-12-2017)

http://www.internetsegura.pt (07-12-2017)

http://www.seguranet.pt (07-12-2017)