PLANO DE SEGURANÇA DIGITAL

Parecer favorável do Conselho Pedagógico de 16 de fevereiro de 2022

PLANO DE SEGURANÇA DIGITAL

1. Introdução

A ESCOLA é um bem público e saber defendê-la passa por saber utilizá-la em condições de eficiência, conforto e segurança.

O presente documento manifesta a preocupação de proporcionar um ambiente e acesso seguros à tecnologia online como parte da experiência de ensino e aprendizagem, para alunos e professores.

Num Mundo cada vez mais tecnológico e virtual/digital, a utilização das tecnologias (telemóveis, computadores, consolas de jogos e a internet) expõe os seus utilizadores a diversas ameaças, deixando-os mais vulneráveis. Assim sendo, hoje, muitas são as crianças, jovens e adultos que interagem, diariamente, com tecnologias e experimentam e vivenciam uma imensurável variedade de oportunidades, atitudes e situações. A troca de ideias, opiniões, experiências, a interação social online e os contextos de aprendizagem daí decorrentes constituem-se como mais-valias para todos, mas, por vezes, os utilizadores ficam expostos a perigos. E, neste sentido, o atual contexto pandémico, evidenciou ainda mais a importância das tecnologias digitais, quer no teletrabalho quer no ensino a distância. A segurança digital não abrange, somente, questões relacionadas com crianças e jovens, mas também com adultos e com a utilização que todos fazem da internet e de todos os dispositivos que permitem a comunicação eletrónica quer em ambientes escolares quer fora deles. Estes contextos exigem a capacitação de todos os elementos da comunidade escolar sobre os riscos e responsabilidades envolvidas e constitui-se como função de cada educador. Todos os educadores e professores devem tomar 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.

A política de segurança digital é, por isso mesmo, essencial na definição de princípios nucleares de ação, que todos os elementos da comunidade escolar devem aplicar.

2. A importância da utilização da internet

A internet revolucionou a nossa forma de comunicação e relacionamento social. Transformou profundamente o modo como interagimos. Alterou o modo como vivemos, aprendemos, trabalhamos, consumimos e nos divertimos. A internet trouxe benefícios na utilização das tecnologias como o fácil acesso ao conhecimento e na colaboração entre as pessoas.

Nos últimos anos novas ferramentas foram criadas para facilitar a criação de conteúdo e compartilhar de maneiras muito simples, seja por meio de blogues, redes sociais, ou vídeos no *YouTube*.

As crianças e os adolescentes são hoje o grupo que mais se destaca na sua utilização. A internet tornou-se muito útil em agregar conhecimento e interatividade. É uma ferramenta muito utilizada na interação social e cada vez mais um aliado no processo de ensino -aprendizagem.

A internet deve fazer parte integrante do currículo como uma ferramenta essencial na aprendizagem, a utilização da internet no Agrupamento deve 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.

Nas atividades de ensino e aprendizagem dever-se-á ensinar aos alunos o que é e o que não é uma utilização aceitável da internet, e ser-lhes-ão indicados objetivos claros, quando utilizam a internet, tendo em conta o currículo e a idade.

A cópia, e a utilização subsequente de materiais obtidos na internet, por alunos e professores, devem cumprir a legislação em matéria de direitos de autor, incluindo o conhecimento dos vários tipos de licenciamentos disponíveis na Web e as regras de utilização dos recursos educativos abertos.

Todas as atividades escolares que impliquem o uso da internet devem permitir aos alunos aprender a pesquisar e a avaliar / validar informação, de acordo com a sua autoria, pertinência e rigor.

2.1. Manutenção da segurança dos sistemas de informação

A segurança dos sistemas informáticos do Agrupamento e dos utilizadores é revista anualmente.

Nos serviços administrativos e na plataforma *Microsoft Teams*, os dados pessoais enviados através da internet ou transferidos para fora da escola estão protegidos pelos sistemas de segurança dos programas utilizados, tendo em conta as recomendações da Comissão Nacional de Proteção de Dados na Deliberação n.º 1495/2016 relativas as restrições de acesso a esses sistemas e à robustez das palavras-chave.

Os dispositivos amovíveis serão utilizados de acordo com as autorizações específicas de cada serviço, estando os sistemas preparados para uma análise automática com antivírus.

Os utilizadores não devem colocar / deixar ficheiros de uso pessoal ou dos alunos nos PC ou nos dispositivos móveis. Após a utilização, nomeadamente para atividades letivas, todos os ficheiros devem ser removidos. Além disso, os utilizadores também devem ter o cuidado de remover todas as contas pessoais associadas a aplicações e não devem, em circunstância alguma, alterar as páginas de navegação pré-definidas.

A capacidade e o funcionamento dos sistemas informáticos são analisados, pelo menos, uma vez por ano letivo.

2.2. Gestão dos conteúdos publicados

As informações de contacto na página Web do Agrupamento devem ser as moradas, os números e telefone e os emails dos vários estabelecimentos do Agrupamento. Não deve ser publicada qualquer informação pessoal de alunos ou professores, exceto quando estas forem obrigatoriamente do domínio público.

A publicitação da listagem dos alunos das turmas só será acessível a alunos e a pais/encarregados e encarregados de educação, mediante registo e em ficheiros protegidos.

Não serão publicadas pautas online e as pautas afixadas em papel nos locais de estilo seguirão as recomendações da Comissão Nacional sobre Proteção de Dados relativas a faltas e outros dados de natureza pessoal.

O Diretor é o responsável editorial geral pelos conteúdos digitais publicados pelo Agrupamento na internet e deve assegurar que os conteúdos publicados são corretos e adequados.

Todas as publicações em formato digital da responsabilidade de membros do Agrupamento devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor e seguir as recomendações da Comissão Nacional de Proteção de Dados no que se refere a identificação ou imagens com alunos.

2.3. Correio eletrónico

A comunicação interna, com alunos, pais/encarregados de educação e com instituições para tratamento de assuntos oficiais do Agrupamento deve ser realizada a partir dos endereços de correio eletrónicos institucionais, disponibilizados pelo Agrupamento.

O reencaminhamento de mensagens em cadeia deve ser evitado e a difusão de informação em grupo dever ser cuidadosa, de modo a evitar ser objeto de *spam*.

O endereço de correio eletrónico institucional não deverá ser utilizado para a criação de contas pessoais em redes sociais.

Os membros da comunidade escolar devem avisar imediatamente a Equipa de Transição Digital se receberem comunicação ofensiva de forma a agir de modo legal e apropriadamente.

2.4. Publicação de fotografias e de trabalhos de alunos

Antes da publicação de imagens ou de gravações vídeo que incluam alunos, deve ser garantida a autorização expressa e informada, de acordo com a legislação aplicável.

A captação de imagens dos alunos deve, preferencialmente, ser executada de longe ou de ângulos que reduzam significativamente a possibilidade de identificação.

Os professores não devem recolher imagens ou voz dos alunos com os seus dispositivos pessoais e não podem publicar diretamente imagens ou outros registos dos alunos nas suas redes sociais pessoais.

Os trabalhos de alunos só serão publicados com a autorização dos mesmos ou dos pais/encarregados de educação.

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

Através de atividades dinamizadas pelos professores em sala de aula e pelo Serviço das Bibliotecas Escolares, os alunos serão ensinados a usar a internet e as redes sociais, de modo a protegerem a sua privacidade, a evitarem a divulgação de dados pessoais, a negarem o acesso a desconhecidos e a bloquearem comunicações não desejadas

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

Os blogues ou *wikis* oficiais geridos pelos professores devem estar protegidos por palavra-passe.

Através da página *Web* do Agrupamento *e* da Biblioteca Escolar do Agrupamento são disponibilizados aos pais/encarregados de educação materiais relacionadas com a utilização de redes sociais, meios sociais e sítios de publicação pessoal (dentro ou fora da escola), especialmente para os alunos mais novos. Ações de sensibilização para o uso seguro da internet podem vir a ser organizadas em colaboração com as Associações de pais/encarregados de Educação do Agrupamento.

2.6. Gestão de telemóveis e outros equipamentos pessoais

Em sessões de sensibilização e atividades dirigidas a alunos dos 5.º e 7.º anos, dinamizadas, quando possível, em articulação entre a Escola Segura, o Serviço das Bibliotecas do Agrupamento e atividades curriculares, os alunos serão instruídos quanto à utilização segura e adequada de telemóveis e outros equipamentos pessoais e serão sensibilizados para os limites e consequências dos seus atos.

Os telemóveis ou equipamentos pessoais podem ser utilizados durante as aulas ou tempos letivos formais para efeitos pedagógicos devidamente autorizados, orientados e supervisionados pelo professor, caso contrário, têm de estar guardados e desligados.

A função de *Bluetooth* dos telemóveis deve estar sempre desligada e não pode ser utilizada para enviar imagens ou ficheiros para outros telemóveis ou para interferir com o funcionamento de outros dispositivos.

3. Resolução de incidentes relativos à segurança digital

Todos os elementos do Agrupamento deverão informar a Direção, se tiverem conhecimento de situações preocupantes, do ponto de vista da segurança digital (tais como violações do sistema de filtragem, *cyberbullying*, conteúdos ilícitos, utilização inadequada de equipamento, …).

A Direção registará todos os incidentes, bem como todas as medidas aplicadas, e tomará as providências necessárias nos casos de cyber*bullying*.

A aplicação de medidas para superação de problemas relativos à Segurança Digital, incluindo os que possam implicar a aplicação de medidas disciplinares, deve ser articulada com os responsáveis pelos serviços onde ocorreram os problemas.

Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal, o Agrupamento contactará a Equipa de Proteção de Menores, através da Direção, e encaminhará a situação para a Escola Segura.

3.1. Gestão dos casos de *cyberbullying*

O *cyberbullying* não será tolerado e todos os incidentes detetados serão comunicados à Direção e às autoridades competentes, sempre que for necessário.

Os alunos do 5.º e 7.º anos terão sessões, dinamizadas pelos Serviços das Bibliotecas Escolares / Escola Segura, em que serão sensibilizados para as questões do *cyberbullying*.

Todos os incidentes de *cyberbullying* comunicados serão registados e serão investigados, aplicando-se, quando necessário, os procedimentos de inquirição usados nos processos disciplinares, tal como estabelecido no Regulamento Interno.

De modo a informar e tornar os nossos alunos mais atentos e sensíveis a este tema, cada turma, deverá eleger, no início do ano letivo, um aluno da turma, com perfil adequado, que assumirá as funções de Embaixador Digital. Caberá a esse aluno, em articulação com a Equipa da Biblioteca Escolar Agrupamento, dinamizar uma sessão anual sobre Segurança Digital e *Cyberbullying*, utilizando os recursos e materiais disponibilizados pela Biblioteca Escolar, e partilhar com os colegas recursos digitais que possam ser utilizados no processo de ensino – aprendizagem.

4. Divulgação do Plano de Segurança Digital à comunidade educativa

O Plano de Segurança Digital está disponível, para conhecimento e consulta, no sítio *Web* do Agrupamento.

No sítio *Web* do Serviço das Bibliotecas do Agrupamento são disponibilizados recursos de apoio para uma utilização segura e responsável da internet e de equipamentos informáticos.

O Agrupamento pretende divulgar aos pais/encarregados de educação o Plano de Segurança Digital em colaboração com os Diretores de Turma e no seu sítio *Web* do Agrupamento.

Por último…

… conhecer os riscos associados à navegação na internet será sempre a melhor forma de precaver acidentes, seja em contexto profissional ou pessoal. Informar e sensibilizar é o primeiro passo para promover uma cultura de segurança, onde todos são conscientes da gravidade que os seus atos podem tomar. E se esta é a regra nº1, podemos assumir que a regra nº 2 é: "*não, não vamos ganhar iphones por sermos selecionados em passatempos*!".

Para mais informações consultar: https://www.seguranet.pt/pt/selo-de-seguranca-digital

5. Algumas recomendações

Antivírus e *Firewall*

Um antivírus, e outros programas que detetam *malware* nos dispositivos, são altamente essenciais para controlar as ameaças. A firewall é igualmente muito importante, uma vez que vai examinar os dados que entram na rede, garantido que são legítimos e, os que não são, acabam filtrados.

Backdoor

É um *software* malicioso que "abre portas" para a entrada de outras ameaças. Uma vez que oferece acesso remoto ao hacker, é muitas vezes difícil de ser identificado e o ataque acontece em segundo plano, permitindo, por exemplo, desvendar palavras-passe, porque o atacante tem autonomia completa no computador.

Backups

Um sistema de *backup* pode prevenir muitas dores de cabeça quando os dados são comprometidos, uma vez que armazena informação em segurança.

DDoS

Este é o tipo de ataque que pretende comprometer o normal funcionamento de um site ou servidor, aproveitando os limites de capacidade específicos que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de uma empresa. Normalmente conhecidos como "redes zombies", são os meios utilizados para sobrecarregar a vítima, que acedem ao site ao mesmo tempo até o serviço ficar instável ou indisponível.

Passwords

Relativamente a *passwords,* a regra mais básica é aquela que, por norma, é menos cumprida: nunca deve ser usado o mesmo acesso para diversos sistemas, muito menos em contexto pessoal e profissional. É importante evitar datas óbvias, como aniversários, e é essencial escolher *passwords* fortes, ou seja, combinações de números, letras e sinais de pontuação. Outro cuidado, para melhorar a segurança a este nível, é desativar o preenchimento automático para utilizadores e senhas.

Phishing

Sendo o tipo de ataque virtual mais comum, o *Phishing* consiste no envio de mensagens de fraude, através de *emails* ou SMS, por exemplo, dando uma falsa sensação de segurança ao

utilizador, porque tenta assemelhar-se a fontes credíveis. O resultado esperado é o roubo de dados confidenciais, como é o caso de acessos a cartões de crédito.

Ransomware

Sendo também dos ataques mais comuns, e que mais danos cria nos dias de hoje, o *Ransomware* é um tipo de *software* mal-intencionado, que mantém refém informações importantes, através do bloqueio de dados. Criado com o intuito de roubar dinheiro, quando os usuários são confrontados com a falta de acesso a arquivos ou sistemas do computador, o atacante pede um resgate. Por norma, mesmo que o dinheiro seja enviado, o bloqueio continua a existir ou os dados foram completamente comprometidos.

Spyware

Tal como o nome indica, este é um *software* que vigia o comportamento do utilizador e pode infetar qualquer dispositivo e dar acesso total a informações confidenciais, como *passwords* ou dados bancários.

Trojans

Os famosos cavalos de Tróia digitais podem comportar-se de formas diferentes, dependendo da intenção do atacante. Um *Trojan* é então uma estratégia de disseminação que os *hackers* utilizam para difundir qualquer tipo de ameaça, desde *ransomware* que imediatamente exige dinheiro, até *spyware* que se esconde enquanto rouba informações valiosas, como dados pessoais e financeiros.

***WiFi* de porta fechada**

Muitas vezes esquecida, a segurança relativa a uma rede *WiFi* pode comprometer a segurança tanto de uma empresa como em casa. Algumas medidas importantes passam por trocar o nome da rede após a instalação do serviço, mudar a *password* de forma regular e desativar o WPS (*Wifi Protected Setup*), obrigando a usar sempre password para aceder á ligação.

Worm

Apesar de não criar danos ao computador, consegue diminuir a velocidade dos equipamentos. Replicando-se em grandes quantidades, consegue transferir informações pela internet, ou até mesmo, para outro computador.