REGULAMENTO DE SEGURANÇA DIGITAL

eSafety

Agrupamento de Escolas de S. Martinho

AGRUPAMENTO
S. MARTINHO

Índice

I - REGULAMENTO DE SEGURANÇA DIGITAL

A *sociedade enfrenta atualmente novos desafios, decorrentes de uma globalização e desenvolvimento tecnológico em aceleração, tendo a escola de preparar os alunos, que serão jovens e adultos em 2030, para empregos ainda não criados, para tecnologias ainda não inventadas, para a resolução de problemas que ainda se desconhecem. (preâmbulo do DL 55/2018, de 6 de julho)*

(1)Objetivos e âmbito do Regulamento de Segurança Digital

1. No Agrupamento de Escolas de S. Martinho (AESM) acredita-se que a segurança digital (eSafety) é um elemento essencial de salvaguarda das crianças, jovens e adultos no mundo digital, ao usar tecnologia, como computadores, *tablets* ou telemóveis.
2. No AESM considera-se que a Internet e as tecnologias de informação e comunicação são uma parte importante da vida quotidiana, pelo que os alunos devem ser apoiados para serem capazes de aprender a desenvolver estratégias de gestão e resposta ao risco *online*.
3. No AESM a direção tem o dever, de acordo com os seus conhecimentos técnicos e disponibilidade de recursos, de proporcionar à comunidade docente pontos de acesso à Internet de qualidade para elevar os padrões de educação, promover a realização de atividades, diversificar as metodologias de ensino, apoiar o trabalho profissional, implementar o projeto dos manuais digitais e melhorar as funções de gestão.
4. No AESM identifica-se que há uma clara obrigação de garantir que todos os alunos, assistentes operacionais e técnicos estão protegidos dos potenciais perigos *online*.
5. Os objetivos do Regulamento de Segurança Digital do agrupamento são:
    a) Identificar claramente os princípios fundamentais, seguros e responsáveis, esperados de todos os membros da comunidade em relação à tecnologia, como forma de garantir um ambiente seguro no que concerne à utilização de equipamentos e da Internet.
    b) Sensibilizar todos os membros para os potenciais riscos, bem como para os benefícios da tecnologia.
    c) Permitir que todos os docentes, assistentes operacionais e técnicos possam trabalhar com segurança e responsabilidade, com vista a um modelo comportamental positivo *online*, estando cientes da necessidade de gerir os seus próprios padrões e práticas ao usar a tecnologia.

- Identificar procedimentos claros a adotar de forma a responder às preocupações de segurança *online* que são conhecidos por todos os membros da comunidade.

6. O regulamento de Segurança Digital aplica-se a todos os docentes, técnicos, assistentes operacionais e técnicos e outras pessoas que trabalham para ou prestam serviços em nome do agrupamento, bem como alunos e pais ou encarregados de educação.
7. Este regulamento aplica-se a todos os dispositivos de acesso à Internet e utilização de dispositivos de comunicação e informação, incluindo dispositivos pessoais, ou outros que tenham sido fornecidos a alunos, funcionários ou outras pessoas.
8. Este regulamento deve ser lida em conjunto com outras políticas escolares relevantes, incluindo proteção da criança, *antibullying*, segurança de dados, uso de imagem e Regulamento de Utilização Aceitável.

II - PRINCIPAIS RESPONSABILIDADES

(1)Competências da Direção

1. Desenvolver e promover uma visão e cultura de segurança *online* para todas as partes envolvidas, em linha com as recomendações nacionais e locais, apoiando e consultando adequadamente toda a comunidade escolar.
2. Garantir que a segurança *online* é vista proactivamente por toda a comunidade como uma questão de salvaguarda.
3. Assegurar que todos os membros da equipa recebem formação regular e adequada quanto à segurança e responsabilidades *online* e orientações relativas a comunicações seguras e adequadas.
4. Tomar conhecimento e decidir acerca de quaisquer incidentes de segurança *online*.

(2)Competências da Equipa PADDE

1. Agir como um ponto de contacto e ligação com outros membros do pessoal docentes e não docente em relação a todas as questões de segurança *online*.
2. Manter-se atualizado sobre legislação e tendências em matéria de segurança *online*.
3. Coordenar a participação em eventos locais ou nacionais para promover o comportamento *online* positivo, por exemplo, o Dia da Internet Segura, bem como a realização de eventos formativos internos.
4. Garantir que a segurança *online* é promovida para os pais e encarregados de educação e a comunidade em geral, através de uma variedade de canais e de abordagens.
5. Trabalhar com o agrupamento para a proteção e segurança de dados, de forma a garantir que a prática está de acordo com a legislação vigente.

6. Monitorizar as definições de segurança *online* para identificar as lacunas e usar esses dados para atualizar a resposta do agrupamento a essas necessidades.
7. Trabalhar com a direção na revisão e atualização do Regulamento de Segurança Digital e Regulamento de Utilização Aceitável.

(3) Pessoal Docente, Pessoal Não Docente, Alunos, Encarregados de Educação

a) **As principais responsabilidades para todos os membros (pessoal) são:**

1. Contribuir para o desenvolvimento do Regulamento de Segurança Digital.
2. Ler os Regulamentos de Utilização Aceitável, aceitando-as, cumprindo-as e fazendo- as cumprir.
3. Assumir a sua responsabilidade individual pela segurança dos sistemas eletrónicos do agrupamento.
4. Ter consciência de uma variedade de diferentes questões relacionadas com a segurança *online* e como elas podem afetar os alunos.
5. Apresentar boas práticas na utilização das novas tecnologias.
6. Incorporar a educação para a segurança *online* no currículo, sempre que possível.
7. Ser capaz de sinalizar, para o apoio adequado disponível, as questões de segurança
8. Manter um nível de conduta profissional no uso pessoal da tecnologia, dentro e fora do local de trabalho.

b) **As principais responsabilidades dos alunos são:**

1. Contribuir positivamente para o desenvolvimento das políticas de segurança *online*.
2. Ler ou pedir que lhes sejam lidas as PUAs e respeitá-las.
3. Respeitar os direitos dos outros, tanto *online* como *offline*.
4. Procurar a ajuda de um adulto de confiança, em caso de necessidade, e apoiar outros alunos que possam estar a enfrentar problemas de segurança *online*,
5. A um nível que é adequado à sua idade, capacidades e vulnerabilidades:
   a. Assumir a responsabilidade de manter a sua segurança e a dos outros *online*.
   b. Assumir a responsabilidade, pela sua própria consciência e aprendizagem, em relação às oportunidades e riscos decorrentes das tecnologias novas e emergentes.
   c. Avaliar os riscos pessoais do uso de qualquer tecnologia específica e comportar-se de forma segura e responsável, para limitar esses riscos.

c) As principais responsabilidades dos pais e encarregados de educação são:

1. Ler o Regulamento da Utilização Aceitável do agrupamento, incentivando os seus filhos ou educandos à sua adesão, e aderindo eles próprios, se for o caso.
2. Discutir questões de segurança *online* com os seus filhos, apoiando o agrupamento nas suas abordagens sobre o tema, reforçando comportamentos *online* seguros e adequados em casa.
3. Ser um modelo apropriado na utilização racional da tecnologia e na adoção de comportamentos seguros *online*.
4. Identificar mudanças no comportamento que possam indicar que o seu filho ou educando está em risco de dano *online*.
5. Procurar ajuda e apoio do agrupamento, ou de outros órgãos competentes, se os seus filhos ou educandos encontrarem problemas ou preocupações *online*.

III - ENSINO, AVALIAÇÃO E APRENDIZAGEM

(1)Importância da Internet

1. A utilização da Internet faz parte integrante do currículo formal sempre que possível e é uma ferramenta essencial na aprendizagem, mais ainda quando o Agrupamento está inserido no projeto dos manuais digitais e é pioneiro na implementação de práticas de gestão digital.
2. Os alunos utilizam a Internet amplamente fora da escola e devem saber como avaliar a informação que obtêm na Internet e como se podem proteger.
3. A finalidade da utilização da Internet no agrupamento é elevar os padrões educativos, diversificar as metodologias de ensino e promover o sucesso dos alunos, apoiar o trabalho dos professores e reforçar a administração escolar.

(2) Benefícios da utilização da Internet no ensino

1. Os benefícios da utilização da Internet no ensino incluem:
   a) Utilização de metodologias híbridas de ensino.
   b) Maximização das vantagens da utilização dos manuais digitais.
   c) Acesso a recursos pedagógicos e educativos de todo o mundo, incluindo museus, simuladores e galerias de arte.
   d) Intercâmbio cultural e educativo entre alunos de várias escolas e realidades.
   e) Utilização social, recreativa e de lazer nas bibliotecas, nos clubes e em casa.

f) Acesso de alunos e professores a peritos em inúmeras áreas.

g) Desenvolvimento profissional dos professores através do acesso a informação, materiais pedagógicos e aplicações eficazes do currículo.

h) Colaboração no âmbito de redes de escolas, serviços de apoio e associações profissionais.

i) Maior acesso a apoio técnico, designadamente gestão remota de redes e atualizações automáticas de programas.

j) Possibilidade de aprendizagem quando e onde for mais conveniente.

(3) Formas de a Internet melhorar a avaliação e a aprendizagem

1. O acesso à Internet do agrupamento será pensado com vista a alargar e reforçar a educação.
2. O agrupamento assegurará que a utilização de materiais obtidos na Internet por alunos e professores cumprem a legislação em matéria de direitos de autor (especialmente licenças CC), incluindo o conhecimento dos vários tipos de licenciamentos disponíveis na web, sendo desenvolvidas diversas campanhas para a defesa dos direitos de autor e implementadas atividades para as fomentar.
3. Os níveis de acesso à Internet serão revistos de modo a corresponderem aos requisitos do currículo e à idade e capacidades dos alunos.
4. Os professores atribuirão aos alunos atividades com recurso à Internet que estejam de acordo com os objetivos de aprendizagem e com a sua idade e capacidades, nomeadamente atividades relacionadas com a utilização dos manuais digitais.
5. Os alunos aprenderão a utilizar eficazmente a Internet para fins de pesquisa, designadamente desenvolver competências de procura, obtenção e avaliação de informações.
6. Os alunos devem aprender como indicar as fontes das informações utilizadas e a respeitar os direitos de autor quando utilizam material obtido na Internet nos seus trabalhos escolares.

(4)Avaliação de conteúdos digitais

1. Deve-se ensinar os alunos a serem críticos em relação aos materiais que leem e a saber como validar uma informação antes de aceitar a sua exatidão.
2. Deve-se orientar os alunos para o uso de ferramentas de pesquisa, adequadas à sua idade.
3. A avaliação de materiais da Internet faz parte do processo de ensino e de aprendizagem de qualquer disciplina e será considerada um requisito transversal à escola e ao currículo e uma

responsabilidade do professor, de acordo com o perfil do aluno à saída da escolaridade obrigatória.

(5)Educação para a Segurança na Internet

1. O AESM disponibiliza um currículo de segurança *online*, através das aulas de TIC nos 2º e 3º ciclos. Para além do currículo, este assunto é explorado transversalmente, de forma a aumentar a consciencialização sobre a importância da utilização segura e responsável da Internet entre os alunos. Nesse sentido a utilização segura e responsável da Internet e da tecnologia em geral deverá, no entanto, ser reforçada em todo o currículo e em todas as áreas.
2. A educação sobre o uso seguro e responsável deverá anteceder o acesso à Internet.
3. Os alunos serão apoiados na leitura e compreensão da Regulamento de Utilização Aceitável para que esta se adapte à sua idade e capacidades.
4. Todos os utilizadores deverão ser informados e estar conscientes de que o uso da Internet será monitorizado.
5. Os utilizadores deverão ser informados de que o tráfego de Internet pode ser monitorizado e rastreado. A descrição e conduta profissional são essenciais ao utilizar os sistemas e dispositivos do agrupamento.
6. Todos os membros do pessoal docente e não docente devem estar cientes de que o seu comportamento *online* fora da escola pode ter um impacto sobre o seu papel e reputação dentro da escola.
7. Os membros do pessoal com a responsabilidade de gerir sistemas de filtragem ou monitorizar o uso das TIC serão supervisionados pela direção e Equipa PADDE e terão procedimentos claros para relatar problemas ou preocupações.

IV - COMUNICAÇÃO ONLINE E UTILIZAÇÃO SEGURA DA TECNOLOGIA

(1) Website

1. Os detalhes de contacto no *site* escolar apenas poderão ser o endereço físico do agrupamento, hiperligações autorizadas, endereço de correio eletrónico oficial e número de telefone.
2. Nenhuma informação pessoal dos alunos deverá será publicada.

3. A direção assumirá a responsabilidade editorial global pelo conteúdo *online* publicado e garantirá que as informações são precisas e adequadas.
4. O *site* cumprirá as orientações do agrupamento para publicações, incluindo a acessibilidade, o respeito pelos direitos de propriedade intelectual, políticas de privacidade e de direitos de autor.
5. Os trabalhos, imagens ou vídeos dos alunos serão publicados com a permissão dos pais ou encarregados de educação.
6. O agrupamento irá postar informações sobre a salvaguarda, incluindo a segurança *online*, no sítio oficial do agrupamento, para os membros da comunidade, incluindo esta Regulamento de Segurança Digital.

(2)Publicação de imagens, vídeos, atividades ou trabalhos dos alunos online

1. O AESM tem uma política clara relativamente à utilização de imagens de alunos onde se definem regras e procedimentos. No início do ano, todos os EE assinam a permissão para o efeito.
2. O agrupamento garantirá que todas as imagens e vídeos compartilhados *online* serão utilizados de acordo com Regulamento de Utilização de Imagem do AESM e carregados em servidores próprios do agrupamento.
3. O AESM garantirá igualmente que todo o uso de imagens, vídeos ou outro material digital se realizará em conformidade com outras políticas e procedimentos, incluindo a segurança e proteção dos dados, Regulamentos de Utilização Aceitável e códigos de conduta.
4. Em linha com a política de imagem, a autorização por escrito dos pais e encarregados de educação será sempre obtida antes das imagens/vídeos de alunos serem publicados *online*.
5. Os nomes completos dos alunos não serão utilizados em parte alguma do *site* do agrupamento, em especial junto a fotografias.

(3)Gestão do correio eletrónico

1. É atribuída uma conta de email institucional a todos os funcionários do AESM para fins profissionais que apenas está ativada durante a permanência do funcionário na instituição, sendo eliminada no momento da sua saída.
2. No primeiro ano de matrícula no AESM é atribuída a cada aluno uma conta de email institucional que terá a duração igual à da permanência do aluno na instituição. Esta conta será utilizada para fins pedagógicos e administrativos.

3. A comunicação com alunos, pais / encarregados de educação e com instituições para tratamento de assuntos oficiais do AESM deve ser preferencialmente realizada a partir de endereços eletrónicos institucionais.
4. As mensagens de correio eletrónico enviadas para organizações externas devem obedecer a procedimentos de escrita e de protocolo similares aos do envio de ofícios por correio físico.
5. 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.

(4)Utilização segura e adequada, em contexto de sala de aula, da Internet

1. A utilização da Internet é uma característica fundamental de acesso à educação e todos os alunos receberão orientação adequada à sua idade e capacidades, de forma a apoiar e permitir desenvolver estratégias de aquisição de um currículo escolar integral e inclusivo.
2. Os níveis de acesso à Internet serão revistos para refletir as exigências curriculares e a idade e capacidade dos alunos.
3. O acesso à Internet é fundamental para que os alunos possam usufruir de todas as funcionalidades dos manuais digitais.
4. Todos os professores devem estar cientes de que não podem contar exclusivamente com os sistemas de filtragem para proteger os alunos e que a supervisão, gestão de sala de aula e educação sobre uso seguro e responsável é essencial e da sua responsabilidade.
5. Os alunos deverão desenvolver atividades *online/offline,* com recurso a ferramentas adequadas, de acordo com a sua idade, e sempre com a supervisão do professor.
6. Todos os dispositivos do agrupamento serão utilizados de acordo com o respetivo Regulamento de Utilização Aceitável e com a segurança apropriada.
7. Os professores deverão, previamente, analisar e avaliar os *sites*, ferramentas e aplicativos de uso em sala de aula ou a recomendar para uso em casa.
8. A avaliação dos materiais disponíveis *online* é uma parte do processo de ensino e aprendizagem em todas as disciplinas e será visto como um requisito em todo o currículo.
9. O AESM tomará todas as medidas necessárias para que a utilização da Internet seja realizada num ambiente seguro.

(5) Telemóveis e equipamentos pessoais

1. O envio de mensagens ou conteúdos abusivos ou inadequados, através de telemóveis ou equipamentos pessoais por parte de qualquer elemento da escola, é proibido e quaisquer violações deste princípio serão tratadas em conformidade com a política de disciplina e de conduta do agrupamento.

2. Não é autorizado o uso de telemóveis e equipamentos pessoais em determinadas áreas dentro da escola, como vestiários, casa de banho ou outras devidamente comunicadas, de acordo com o Regulamento Interno.
3. Não é permitido levar telemóveis e outros equipamentos para os exames e / ou outras provas de avaliação. Os alunos que tenham um telemóvel na sua posse durante um exame estarão sujeitos às normas estabelecidas pelo Júri Nacional de Exames.
4. Os professores podem confiscar um telemóvel ou equipamento se se considerar que está a ser utilizado de modo contrário às políticas do agrupamento em matéria de conduta ou *bullying*, de acordo com o Regulamento Interno.
5. A direção pode fazer uma pesquisa ao telemóvel ou equipamento com o consentimento dos pais ou encarregados de educação. Caso se suspeite que o equipamento pessoal contém materiais que podem constituir prova de uma ação ilícita, o telemóvel será entregue à polícia para averiguações.
6. Os professores e restante pessoal são responsáveis pelos dispositivos eletrónicos de todos os tipos que tragam para a escola.
7. O AESM não assume qualquer responsabilidade pela perda, roubo ou dano de tais objetos, nem por quaisquer efeitos prejudiciais para a saúde causados por estes dispositivos, sejam eles reais ou potenciais.

(6)Utilização de equipamentos pessoais pelos alunos

1. Se um aluno violar as políticas do agrupamento, o seu telemóvel ou equipamento será apreendido e guardado em local seguro na escola, de acordo com o Regulamento Interno. Os telemóveis e outros equipamentos pessoais serão entregues aos pais ou encarregados de educação, em conformidade com as políticas do agrupamento.
2. Se um aluno necessitar de contactar os pais, deverá informar um professor ou assistente operacional que realizará o contacto, utilizando os meios oficiais da escola.
3. Os alunos devem proteger os seus números de telefone, dando-os a conhecer apenas a amigos e familiares de confiança. 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.
4. Os alunos não estão autorizados a utilizar telemóveis nos locais onde decorram aulas ou outras atividades formativas, exceto quando a utilização de qualquer dos meios acima referidos esteja diretamente relacionada com as atividades a desenvolver e seja expressamente autorizada pelo professor, pelo responsável pela direção ou pela supervisão dos trabalhos ou atividades em curso, de acordo com o Regulamento Interno.

5. Durante o período letivo, os telemóveis e outros equipamentos deverão estar desligados ou em modo de "silêncio". Os referidos equipamentos não serão utilizados em períodos letivos, exceto em emergências autorizadas pela direção.
6. Se, por motivos pedagógicos, os professores pretenderem que os alunos utilizem telemóveis ou outros equipamentos pessoais numa atividade educativa, isso será feito com a aprovação da direção e de acordo com este Regulamento de Segurança Digital.

V - REDES SOCIAIS

(1) Disposições gerais

1. A utilização segura e responsável dos meios de comunicação social, nomeadamente as redes sociais, será preocupação de todos os membros do AESM, como forma de proteger a comunidade em geral, *online* e *offline*. Podem incluir-se nas redes sociais: *blogues*, *wikis*, *sites* de redes sociais, fóruns, painéis de mensagens, jogos *multiplayer online*, aplicativos de vídeo/*sites* de partilha de fotos, *chats*, mensagens instantâneas e outros.
2. Todo o pessoal do AESM será incentivado a envolver-se nas *redes* sociais de uma maneira positiva, segura e responsável, em todos os momentos.
3. Todo o pessoal do AESM, incluindo alunos, é aconselhado a não publicar detalhes específicos e privados, pensamentos, preocupações, imagens ou mensagens em quaisquer serviços de *rede* social, especialmente conteúdo que possa ser considerado ameaçador, prejudicial ou difamatório aos outros ou para com a instituição.
4. O AESM reserva-se o direito de controlar e/ou vedar o acesso de alunos e restante pessoal às diversas redes sociais e *sites* de redes sociais, quando realizado no local e se resultar do uso de dispositivos ou sistemas escolares.
5. O uso de aplicações de redes sociais durante o horário escolar para uso pessoal não é permitido (excetua(m)-se o(s) período(s) de descanso devidamente autorizado(s) e nos locais apropriados).
6. O uso inadequado ou excessivo das redes sociais durante o horário de trabalho ou através do uso de dispositivos escolares pode resultar em ação disciplinar ou legal e/ou remoção de recursos da Internet.
7. Quaisquer preocupações relativas à conduta *online* de qualquer membro do AESM em *sites* de *redes* sociais devem ser comunicadas à direção e serão geridas em conformidade com as políticas do agrupamento.

8. Quaisquer violações das políticas explícitas do agrupamento podem resultar em ações criminais, disciplinares ou civis, tendo em consideração a idade e a função dos envolvidos e as circunstâncias do erro cometido.

(2)Uso oficial das redes sociais

1. O uso oficial das redes sociais pelo agrupamento visa exclusivamente o trabalho educacional, através da divulgação ou comunicação destinada, por exemplo, a aumentar o envolvimento dos pais e encarregados de educação.
2. Os canais oficiais da agrupamento nas redes sociais deverão ser configurados de forma segura, sóbria e institucional, destinando-se exclusivamente a fins educativos e a uma utilização responsável, de acordo com a legislação local e nacional.
3. Toda a comunicação nas plataformas oficiais deve ser clara, transparente e aberta ao escrutínio, nomeadamente no *teams*.
4. Qualquer publicação *online* em *sites* oficiais ou de *rede* social deverá cumprir os requisitos legais, incluindo a Lei de Proteção de Dados, o direito à privacidade ou a obrigação em proteger informação privada e não deverá violar qualquer dever de direito comum de confidencialidade, direitos de autor, *Cyberbullying*, etc.
5. Imagens, vídeos ou trabalhos de alunos só serão compartilhadas em *sites* de *rede* social, canais oficiais ou redes sociais de acordo com o Regulamento de Privacidade e Proteção de Dados Pessoais.
6. Pais e encarregados de educação, alunos, professores e restante pessoal serão informados da existência dos diversos canais oficiais e do respetivo Regulamento de Privacidade e Proteção de Dados Pessoais.
7. O(s) responsável(eis) que gerem os canais oficiais do agrupamento, nomeadamente as redes sociais, não devem divulgar informações, fazer compromissos ou participar em atividades em nome do agrupamento, a menos que estejam devidamente autorizados a fazê-lo.
8. É proibida a comunicação direta com pais, encarregados de educação ou alunos através de qualquer canal de rede social (deve ser apenas utilizado o *teams*, o *email* institucional ou carta registada).
9. Os membros do pessoal docente e não docente serão incentivados a gerenciar e controlar, de forma responsável, o conteúdo que partilharem e publicarem *online*.
10. Os professores que pretendam utilizar ferramentas das redes sociais com os alunos, em atividades curriculares, avaliarão o risco dos sítios na Internet antes de os utilizar e verificarão os termos e condições dos mesmos, de modo a garantir que são adequados às idades dos alunos. Adicionalmente, os professores poderão obter aconselhamento da direção ou da Equipa PADDE antes de utilizarem redes sociais na sala de aula.

11. As opiniões pessoais do pessoal não refletem nem vinculam a posição oficial do agrupamento como instituição.

(3) Uso pessoal das redes sociais

1. A publicação pessoal em *sites* de media social será ensinada aos alunos, como parte de uma abordagem incorporada e progressiva, através de *sites* apropriados à sua idade, que foram alvo de uma avaliação de risco e aprovados como adequados para fins educativos.
2. Os alunos serão aconselhados a considerar os riscos de partilhar detalhes pessoais de qualquer tipo em sites de media social que possam identificá-los ou a sua localização. Exemplos incluem o nome real/completo, endereço, números de telefone móvel ou fixo, escola frequentada, detalhes de contacto, endereços de correio eletrónico, nomes completos dos amigos/família, interesses específicos, etc.
3. Os alunos serão aconselhados a não promover encontros *online* sem a permissão dos pais ou outro adulto responsável e apenas na sua presença.
4. Os alunos serão informados sobre a segurança adequada em sites de *rede* social e serão incentivados a utilizar em segurança senhas, negar o acesso a indivíduos desconhecidos e a aprender a bloquear e relatar comunicações não desejadas.
5. Qualquer atividade de *rede* social oficial, envolvendo alunos no recinto escolar, deverá ser sempre moderada pelo agrupamento.
6. Sempre que solicitado, serão abordadas com os pais ou encarregados de educação questões e preocupações relacionadas com a utilização de redes sociais, meios sociais e sítios de publicação pessoal (dentro ou fora da escola), especialmente quando se trata de alunos mais novos.

VI - GESTÃO DE SISTEMAS DE INFORMAÇÃO

(1)Manutenção da segurança dos sistemas de informação

1. 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.
2. Os utilizadores devem assumir responsabilidade pela utilização da Internet.
3. Os computadores de trabalho devem estar protegidos contra determinadas ações inadvertidas ou deliberadas dos utilizadores.
4. Os computadores de trabalho deverão ter mais do que um navegador de Internet, contendo extensões que permitam bloquear publicidade e navegar de forma privada, incluindo o uso de motores de pesquisa com a inclusão de navegação em privado.
5. Toda a rede interna deve ter instalada e atualizada uma proteção antivírus e *firewall*.

6. O acesso por dispositivos sem fios deve ser administrado proativamente e estar sujeito a um nível de segurança mínimo com encriptação WPA2.
7. A segurança dos sistemas informáticos do agrupamento e dos utilizadores será revista com regularidade.
8. É obrigatória a autenticação para aceder à rede do agrupamento;
9. A proteção antivírus será atualizada com regularidade.
10. As regras da *firewall* devem ser conhecidas e atualizadas de acordo com as ameaças de cibersegurança.
11. Nenhum *Software* não aprovado será autorizado nas áreas de trabalho ou como anexo de mensagens eletrónicas.
12. Os ficheiros guardados na rede do agrupamento ou nos postos de trabalho serão verificados com regularidade.
13. A utilização de nomes de utilizador e palavras-passe para aceder à rede do agrupamento ou aos postos de trabalho deverá ser obrigatória (aplicações de gestão dos alunos e do correio eletrónico, entre outras).
14. Sempre que possível, serão integradas extensões de programas nos navegadores de Internet, (tais como o *Adblock Plus* ou outros semelhantes), o que permitirá a utilização de uma navegação mais privada e com menor índice de publicidade não desejada, durante o uso da *web*.

(2) Sistemas de filtragem

1. O acesso à Internet fornecido pelo agrupamento incluirá sistemas de filtragem adequados à idade e à maturidade dos alunos.
2. Se sítios indesejáveis chegarem ao conhecimento de alunos, professores ou outros, o endereço será comunicado à direção/Equipa PADDE que documentará o incidente.
3. Qualquer material que o AESM considere ilegal será denunciado através dos mecanismos oficiais.
4. A estratégia de acesso à Internet do agrupamento deve ser delineada de forma a estar em consonância com a idade e o currículo dos alunos.
5. O AESM deverá garantir que os sistemas adequados de filtragem e controlo estão implementados, de forma a evitar que pessoal e alunos possam aceder a conteúdo inadequado ou ilegal.
6. O AESM irá tomar todas as precauções razoáveis para garantir que os utilizadores acedam apenas a material apropriado. No entanto, devido à natureza global e conetividade do conteúdo disponível na Internet, nem sempre é possível garantir que o acesso a material inadequado nunca ocorrerá através de uma configuração ou dispositivo escolar.

7. O AESM irá auditar o uso da tecnologia para determinar se o Regulamento de Segurança Digital é adequada e que a sua implementação é apropriada.
8. Os métodos para identificar, avaliar e minimizar os riscos *online* serão revistos regularmente pela direção e pela Equipa PADDE.

VII - REDUZIR OS RISCOS ONLINE

(1)Tecnologias emergentes

1. O AESM está ciente de que a Internet é um ambiente em constante mudança, com novos aplicativos, ferramentas, dispositivos, *sites* e materiais a emergir a um ritmo rápido.
2. Cabe a cada professor examinar e avaliar as tecnologias emergentes de acordo com o seu benefício educacional, solicitando, se necessário, a opinião da direção ou Equipa PADDE.

(2)Autorização e utilização da Internet no recinto escolar

1. Os pais e encarregados de educação deverão ser informados que é fornecido aos alunos acesso supervisionado à Internet, apropriado para a sua idade e capacidades.
2. Os pais e encarregados de educação são convidados a ler/analisar o Regulamento de Utilização Aceitável para o acesso dos alunos, com os seus filhos/educandos.
3. Ao considerar o acesso para os membros vulneráveis da comunidade (nomeadamente, os alunos com necessidades específicas), o agrupamento tomará as decisões com base nas necessidades específicas e compreensão do(s) aluno(s).
4. Os alunos utilizarão apenas um acesso dedicado a eles, com permissões específicas (utilizar aluno 2021):
5. O acesso à rede de Internet do agrupamento está vedado a todos os visitantes, exceto em caso de necessidade extrema e mediante autorização da direção ou da Equipa PADDE, ficando sujeitos a este Regulamento de Segurança Digital e aos restantes Regulamentos de Utilização Aceitável.

(3)Incidentes preocupantes

1. A observação do comportamento dos alunos é essencial na deteção de situações preocupantes e na criação da confiança necessária à partilha, com os professores, de problemas.

2. Todos os elementos do agrupamento serão informados sobre como proceder para comunicar situações preocupantes do ponto de vista da segurança digital (tais como, violações do sistema de filtragem, *Cyberbullying*, conteúdos ilícitos, etc.).
3. A direção e a Equipa PADDE deverão ser informados de todos os incidentes relacionados com segurança digital que envolvam preocupações ao nível da proteção de menores, estes agirão em conformidade, nomeadamente através do contacto das entidades competentes.
4. O agrupamento gerirá os incidentes relacionados com a segurança digital em conformidade com as políticas do agrupamento em matéria de disciplina/conduta, previstas no regulamento interno. Depois de concluídas eventuais investigações, retirará ilações e, se necessário, tomará medidas.
5. O agrupamento informará os pais/encarregados de educação de quaisquer incidentes ou preocupações, quando e como considerar mais adequado.
6. Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal, o AESM contactará a Equipa de Proteção de Menores, o responsável pelas questões de segurança digital ou outra pessoa competente e encaminhará a situação para a polícia.

(4)Denúncias relacionadas com a segurança digital

1. As queixas relativas à utilização indevida da Internet serão tratadas no quadro dos procedimentos de apresentação de queixas ou denúncias adotadas pelo agrupamento, de acordo com o Regulamento Interno.
2. Quaisquer queixas que envolvam a utilização indevida da Internet por pessoal docente, não docente ou restante pessoal serão encaminhadas para a direção.
3. O AESM manterá um registo de todos os incidentes ou queixas relacionadas com a segurança digital, assim como das medidas tomadas.
4. Os professores e os alunos serão informados dos procedimentos necessários para apresentação de queixas e trabalharão em conjunto com o agrupamento, com vista à resolução dos problemas.
5. Quaisquer situações (incluindo sanções) serão tratadas de acordo com os procedimentos do agrupamento em matéria de conduta, disciplina e proteção de menores.

(5)Cyberbullying

1. O *Cyberbullying* pode ser definido como "*A utilização de uma tecnologia, em especial os telemóveis e a Internet, para deliberadamente causar dano ou incomodar alguém*".
2. O *Cyberbullying* (assim como todas as outras formas de *bullying*) de qualquer elemento do agrupamento não será tolerado.

3. De uma forma geral, para dar apoio a qualquer elemento da comunidade escolar que seja alvo de *Cyberbullying,* o agrupamento adotará procedimentos formais semelhantes ao registo de ocorrências de incidentes preocupantes, em documento próprio.
4. Todos os incidentes de *Cyberbullying* comunicados serão registados.
5. Alunos, professores e pais ou encarregados de educação serão aconselhados a manter um registo do *bullying* como prova.
6. O AESM tomará medidas para identificar o responsável pela situação de *bullying*, sempre que possível e adequado. Isto poderá passar pela análise dos registos informáticos do agrupamento, por identificar e entrevistar possíveis testemunhas e contactar o fornecedor do serviço e a polícia, se necessário.
7. Será solicitado a alunos, professores e pais ou encarregados de educação que trabalhem em conjunto com o agrupamento, de modo a apoiarem a abordagem em relação ao *Cyberbullying* e à segurança digital.
8. As sanções para os envolvidos em *Cyberbullying* podem incluir o seguinte:
   a. O autor poderá ter de retirar a publicação de todo o material considerado inapropriado. Para o efeito, em caso de recusa ou incapacidade, poderá ser contactado o fornecedor do serviço.
   b. O autor poderá ver suspenso o seu direito de acesso à Internet do agrupamento, durante um determinado período. Poderão ser previstas outras sanções para alunos e professores, em conformidade com as políticas do agrupamento em matéria de conduta e antibullying ou os Regulamento de Utilização Aceitável, de acordo com o estatuto dos alunos e o regulamento interno.
   c. Os pais/encarregados de educação serão informados.
   d. A polícia será contactada caso se suspeite de ação ilícita.

VIII - DISPOSIÇÕES FINAIS

1. O AESM reconhece que os pais e encarregados de educação têm um papel essencial a desempenhar para permitir que as crianças se tornem utilizadores seguros e responsáveis da Internet e da tecnologia digital.
2. Deverá ser incentivada uma abordagem de parceria para a segurança *online* em casa e na escola com os pais e encarregados de educação.
3. O AESM disponibiliza-se, através dos seus responsáveis, a fornecer informação e orientação aos pais e encarregados de educação sobre segurança *online*.

4. Os pais e encarregados de educação deverão ser encorajados a serem um modelo de comportamento positivo para os alunos no que toca à segurança *online*.
5. O AESM chamará a atenção dos pais e encarregados de educação para o seu Regulamento de Segurança Digital através de boletins informativos ou do seu sítio na Internet.
6. Será incentivada uma abordagem de parceria família/escola em relação à segurança digital em casa e na escola. Para esse efeito, poderão ser organizadas sessões com demonstrações e sugestões para uma utilização segura da Internet em casa ou outros eventos direcionados aos pais e encarregados de educação.
7. Será solicitado aos pais que leiam e debatam o Regulamento de Utilização Aceitável e o Regulamento de Segurança Digital do agrupamento, e respetivas implicações, com os seus filhos.
8. O AESM deve ter um Regulamento de Utilização Aceitável consubstanciado num documento claro e conciso, orientador do uso adequado e seguro das novas tecnologias na escola e da utilização de equipamentos tecnológicos.
9. O AESM implementará Regulamentos de Utilização Aceitável, com o intuito de proteger alunos, professores e outros elementos.
10. Todos os membros do agrupamento deverão estar informados sobre o processo de comunicação das preocupações de segurança *online* (eSafety), tais como violações de filtragem, *sexting*, *Cyberbullying*, conteúdo ilegal, entre outras.
11. A direção deverá ser informado de qualquer incidente de segurança *online* envolvendo preocupações de proteção da criança.
12. Todos os membros da comunidade escolar devem estar cientes dos comportamentos seguros e adequados *online* e da importância de não publicar qualquer conteúdo, comentários, imagens ou vídeos que causem danos, angústia ou ofensa a quaisquer outros membros da comunidade escolar.
13. O AESM deverá informar os pais e encarregados de educação de quaisquer incidentes ou preocupações relativas aos alunos, como e quando necessário.
14. Depois de identificados os possíveis incidentes, o agrupamento deve implementar as alterações, conforme necessário.
15. Pais, encarregados de educação, alunos e restante pessoal têm a obrigação de trabalhar em parceria com o agrupamento de forma a resolver atempada e satisfatoriamente os problemas surgidos.
16. Serão disponibilizadas informações aos alunos e pais e encarregados de educação sobre recursos úteis e sítios na Internet, sistemas de filtragem e atividades pedagógicas e lúdicas, que abordem uma utilização positiva e responsável da Internet.

17. Qualquer situação omissa nos Regulamentos do agrupamento deverá ser analisada à luz da legislação nacional e das orientações da Comissão Nacional de Proteção de Dados (http://www.cnpd.pt/).