Agrupamento de Escolas

DR. CARLOS PINTO FERREIRA

POLÍTICA DE SEGURANÇA DIGITAL

Escola de excelência, melhor escola, melhores cidadãos

Política de Segurança Digital

Usar a Internet e os dispositivos digitais em segurança

Índice

1. Política de segurança digital

A segurança digital visa proteger a confidencialidade, integridade e disponibilidade de autenticidade de documentos e dados pessoais. Atualmente, crianças, jovens e adultos interagem diariamente com as mais diversas tecnologias (os telemóveis, as consolas de jogos, a Internet, etc…) e contactam, experimentam e vivenciam uma infindável variedade de oportunidades, atitudes e situações. A troca de ideias, opiniões, experiências, a interação social online e as oportunidades de aprendizagem daí decorrentes apresentam enormes benefícios para todos, mas podem, por vezes, colocar crianças, jovens e adultos em perigo.

A segurança digital abrange questões relacionadas não só 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 em ambiente escolar e fora dele. Isto exige a atenção e formação de todos os elementos da comunidade escolar sobre os riscos e responsabilidades envolvidas e faz parte do cuidado inerente à função de cada educador.

Todos os educadores e professores devem, pois, ter 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.

O Coordenador da Política de Segurança Digital é designado pelo diretor e funciona como elemento de articulação com a Direção do Agrupamento de Escolas Dr. Carlos Pinto Ferreira, designado neste documento por AEDCPF.

A política de Segurança Digital, redigida com base na Política do Selo de Segurança Digital e na legislação aplicável, será revista anualmente.

Este documento foi alterado de acordo com o Regulamento Geral de Proteção de Dados (RGPD) que entrou em vigor em 25 de maio de 2018.

31 de agosto de 2020

O/A Coordenador/a da Política de Segurança Digital _____

Política aprovada pelo Diretor _____

2. Objetivos da Política de Segurança

Os objetivos da Política de Segurança Digital (PSD) são:

- Identificar claramente os princípios fundamentais, seguros e responsáveis esperados de todos os membros da comunidade em relação à tecnologia como forma de garantir que a instituição seja um ambiente seguro no que concerne à utilização de equipamentos e da Internet.
- Sensibilizar todos os membros da comunidade educativa sobre os potenciais riscos, bem como dos benefícios da tecnologia.
- Permitir que todos os funcionários 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.

Esta política aplica-se a todos os funcionários, incluindo, professores, pessoal de apoio, prestadores de serviços, visitantes, voluntários e outras pessoas que trabalham para ou prestam serviços em nome da escola (coletivamente e adiante referidos como «pessoal» nesta Política), bem como alunos e pais ou encarregados de educação.

Esta Política 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.

Esta Política deve ser lida em conjunto com outras políticas escolares relevantes, incluindo (mas não limitada à salvaguarda e proteção da criança, antibullying, segurança de dados, uso de imagem, confidencialidade, triagem, busca e confisco e políticas relevantes para o currículo).

3. Principais responsabilidades

3.1. Competências do Órgão de Gestão e da Equipa de Segurança Digital

- 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.
- Garantir que a segurança online é vista proactivamente por toda a comunidade como uma questão de salvaguarda.
- Apoiar o Coordenador de Segurança Digital, garantindo que tenha tempo e recursos suficientes para cumprir o seu papel de segurança online e demais responsabilidades.
- 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.
- Tomar conhecimento e decidir acerca de quaisquer incidentes de segurança online.
- Assegurar que são realizadas avaliações de risco adequadas sobre a utilização segura da tecnologia, incluindo a garantia de uma utilização responsável dos dispositivos.

3.2. Competências do Coordenador de Segurança Digital

- Agir como um ponto de contato e ligação com outros membros do pessoal e outras agências, conforme apropriado, em relação a todas as questões de segurança online.
- Manter-se atualizado com a pesquisa atual, legislação e tendências em matéria de segurança digital e online.

- Coordenar a participação em eventos locais ou nacionais para promover o comportamento online positivo, por exemplo, o Dia da Internet Segura.
- 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.
- Trabalhar com a escola para a proteção e segurança de dados, de forma a garantir que a prática está de acordo com a legislação vigente.
- Monitorizar as definições de segurança online para identificar as lacunas e usar esses dados para atualizar a resposta da escola a essas necessidades.
- Informar a equipa de gestão da escola e outras agências, conforme apropriado, em questões de segurança online.
- Facilitar a ligação com organismos locais e nacionais, conforme apropriado.
- Trabalhar com a Equipa de Liderança na revisão e atualização da Política de Segurança Digital, Políticas de Utilização Aceitável (PUAs), Política de Privacidade e outras políticas relacionadas numa base regular (pelo menos anualmente).
- Garantir que a segurança online é integrada noutras políticas e procedimentos da escola de forma apropriada.

3.3. Pessoal Docente, Não Docente, Alunos, Prestadores de Serviços ou de Apoio

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

- Contribuir para o desenvolvimento da Política de Segurança Digital.
- Ler as Políticas, aceitando-as, cumprindo-as e fazendo-as cumprir.
- Assumir a sua responsabilidade individual pela segurança dos sistemas eletrónicos da escola.
- Ter consciência de uma variedade de diferentes questões relacionadas com a segurança online e como elas podem afetar os alunos sob os seus cuidados.
- Apresentar boas práticas na utilização das novas tecnologias.
- Incorporar a educação para a segurança online no currículo, sempre que possível.
- Identificar situações individuais de preocupação e tomar medidas apropriadas, seguindo as políticas e procedimentos de salvaguarda da escola.
- Ser capaz de sinalizar para o apoio adequado disponível as questões de segurança online, interna e externamente.
- Saber quando e como escalar questões de segurança online, interna e externamente.
- Manter um nível de conduta profissional no seu uso pessoal da tecnologia, dentro e fora do local de trabalho.

As principais responsabilidades dos alunos são:

- Contribuir positivamente para o desenvolvimento das políticas de segurança online.
- Ler ou pedir que lhes sejam lidas as Políticas e respeitá-las.
- Respeitar os sentimentos e os direitos dos outros, tanto online como offline.
- Procurar a ajuda de um adulto de confiança, se as coisas correrem mal, e apoiar outros que podem estar enfrentando problemas de segurança online.

A um nível que é adequado à sua idade, capacidades e vulnerabilidades:

- Assumir a responsabilidade por manter-se a si e aos outros seguros online.
- Assumir a responsabilidade pela sua própria consciência e aprendizagem em relação às oportunidades e riscos decorrentes das tecnologias novas e emergentes.
- Avaliar os riscos pessoais do uso de qualquer tecnologia específica, e comportar-se de forma segura e responsável, para limitar esses riscos.

As principais responsabilidades dos pais e encarregados de educação são:

- Ler as Políticas da escola, incentivando os educandos ao cumprimento.
- Discutir questões de segurança online com os seus filhos, apoiando a escola nas suas abordagens sobre o tema, reforçando comportamentos online seguros e adequados em casa.
- Ser um modelo apropriado na utilização racional da tecnologia e na adoção de comportamentos seguros online.
- Identificar mudanças no comportamento que possam indicar que o seu filho ou educando está em risco de dano online.
- Procurar ajuda e apoio da escola, ou de outros órgãos competentes, se os seus filhos ou educandos encontrarem problemas ou preocupações online.
- Assumir a responsabilidade pela sua própria consciência e aprendizagem em relação às oportunidades e riscos decorrentes das tecnologias novas e emergentes.

4. Ensino e aprendizagem

4.1. A importância da utilização da Internet

- Devendo fazer parte integrante do currículo como uma ferramenta essencial na aprendizagem, a utilização da Internet no AEDCPF 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.
- Os níveis de acesso à Internet serão estabelecidos de acordo com os requisitos do currículo, idade e capacidades dos alunos.
- Todas as atividades escolares que impliquem o uso da Internet devem integrar a apresentação das referências bibliográficas.

4.2. Benefícios da utilização da Internet no ensino

- Acesso a recursos pedagógicos e educativos.
- Intercâmbio cultural e educativo entre alunos de vários países.
- Desenvolvimento profissional dos professores através do acesso a materiais pedagógicos e aplicações eficazes do currículo.
- Maior acesso a apoio técnico, designadamente gestão remota de redes e atualizações automáticas de programas.
- Possibilidade de aprendizagem quando e onde for mais conveniente.

4.3. Utilização da Internet com vista à melhoria da aprendizagem

- O acesso à Internet no AEDCPF deve ser pensado com vista a alargar e reforçar a educação.
- 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.
- 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.
- 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.

4.4. Utilização de Tecnologias em Atividades Letivas/Não Letivas

Utilização de dispositivos tecnológicos e de captura de imagem ou de vídeo no recinto escolar:

- Não utilizar quaisquer equipamentos tecnológicos, designadamente, telemóveis, equipamentos, programas ou aplicações informáticas, nos locais onde decorram aulas ou outras atividades, exceto quando a utilização esteja diretamente relacionada com as atividades a desenvolver e seja expressamente autorizada pelo professor ou pelo responsável pela direção ou supervisão dos trabalhos ou atividades em curso.
- Não captar sons ou imagens, designadamente, de atividades letivas e não letivas ou qualquer atividade dentro do recinto escolar (nomeadamente, no recreio), 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 utilizar auriculares com ou sem fios dentro da sala de aula, sem autorização do docente.
- Não difundir, na escola ou fora dela, nomeadamente, via Internet ou através de outros meios de comunicação, sons ou imagens captadas nos momentos letivos e não letivos, sem autorização do diretor da escola, nomeadamente imagens com outros colegas.

Utilização de dispositivos tecnológicos e de captura de imagem ou de vídeo nas atividades letivas e não letivas on-line:

- Deve ser utilizada a conta de email do domínio @agrupajunqueira.pt (…@agrupajunqueira.pt) para efetuar o registo nas plataformas utilizadas para o desenvolvimento das atividades letivas ou outras necessárias (exemplo o Google Classroom), não sendo aceite outra conta.
- As contas devem ser protegidas, não fornecendo a palavra-passe a terceiros e fazendo logout da mesma sempre que estiver num computador que não seja usado apenas por o mesmo.
- A palavra-passe deve cumprir os requisitos de segurança, nomeadamente, ser constituídas por um mínimo de oito carateres e incluir letras maiúsculas, letras minúsculas, números e carateres especiais (como por exemplo “;.-/”).
- O aluno e o professor devem estar presentes em todas as atividades online, da mesma forma que as suas presenças são requeridas, quando as atividades são dentro do recinto escolar.
- Não devem ser captados sons ou imagens das aulas online.
- Não difundir, na escola ou fora dela, nomeadamente, via Internet ou através de outros meios de comunicação, sons ou imagens captadas em sessões online com professores ou outros responsáveis pertencentes à escola.

Guardar material referente à atividade Letiva

- Os alunos devem guardar todo o material elaborado em aula, na sua conta Google (exemplo: Google Drive), evitando a utilização de dispositivos amovíveis.

4.5. Avaliação de conteúdos

- Deve promover-se nos alunos o espírito crítico em relação aos materiais que leem e a saber como validar uma informação antes de aceitar a sua exatidão.

- A avaliação de materiais da Internet faz parte do processo de ensino e de aprendizagem de qualquer disciplina, sendo considerada um requisito transversal.

5. Gestão de sistemas de informação

5.1. Manutenção da segurança dos sistemas de informação

- A segurança dos sistemas informáticos do AEDCPF e dos utilizadores é revista anualmente.
- A proteção antivírus é atualizada frequentemente.
- Os dados pessoais enviados através da Internet ou transferidos para fora da escola estão protegidos pelos sistemas de segurança lógicos e físicos.
- O/a gestor/a da rede analisa a capacidade e o funcionamento do sistema com regularidade.
- Os dispositivos amovíveis são utilizados de acordo com as autorizações específicas de cada serviço, estando os sistemas preparados para uma análise automática de prevenção.
- Os utilizadores não podem instalar qualquer software. A instalação de software para fins educativos deve ser autorizada pelo Coordenador da Segurança Digital e feita, preferencialmente por ele mesmo ou por quem ele designe.
- Após a utilização, nomeadamente para atividades letivas, todos os ficheiros devem ser removidos.
- A capacidade e o funcionamento dos sistemas informáticos serão analisados, pelo menos, uma vez por ano letivo.
- É obrigatória a autenticação para aceder à rede da escola.
- A página inicial de navegação de cada computador ao serviço dos utilizadores será definida pela de acordo com as necessidades / interesses dos serviços. Os utilizadores não devem, em circunstância alguma, alterar as páginas de navegação pré-definidas.
- De forma a reforçar e evitar as alterações anteriormente mencionadas, os sistemas estão protegidos com permissões por utilizadores.

5.2. Gestão do correio eletrónico

- É atribuída uma conta de email institucional a todos os funcionários do AEDCPF para fins profissionais que apenas está ativada durante a permanência do funcionário na instituição, sendo eliminada no momento da sua saída.
- No primeiro ano de matrícula no AEDCPF 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.
- A comunicação com alunos, pais / encarregados de educação e com instituições para tratamento de assuntos oficiais do AEDCPF deve ser preferencialmente realizada a partir de endereços eletrónicos institucionais.
- 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.
- 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.

5.3. Gestão dos conteúdos publicados

- As informações de contato no sítio do AEDCPF devem ser a morada, os números de telefone e o email do AEDCPF. Não deve ser publicada qualquer informação pessoal de alunos ou

professores.

- O responsável editorial geral pelos conteúdos digitais publicados pelo AEDCPF na Internet é nomeado pelo Diretor e deve assegurar que os conteúdos publicados são corretos e adequados.
- Todas as publicações em formato digital da responsabilidade de membros do AEDCPF devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

5.4. Publicação de fotografias e trabalhos de alunos

- Na publicação de imagens e/ou gravações vídeo que incluam alunos, deve ser garantida a proteção da imagem dos alunos, de acordo com a legislação aplicável.
- Os nomes completos dos alunos não serão utilizados em parte alguma do sítio do AEDCPF, em especial junto a fotografias.
- A publicação de qualquer imagem e/ou vídeo de alunos, será feita apenas, depois de obtida autorização por escrito dos pais e /ou encarregados de educação.
- Os trabalhos de alunos podem ser publicados, desde que não estejam identificados, ou após obtida autorização por escrito dos pais e /ou encarregados de educação.

5.5. 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.

5.6. Gestão dos sistemas de filtragem

- O acesso à Internet fornecido pelo AEDCPF inclui sistemas de filtragem adequados à idade e à maturidade dos alunos.
- A estratégia de acesso à Internet da escola pode ser delineada de forma a estar em consonância com a idade e o currículo dos alunos.
- Se sítios indesejáveis chegarem ao conhecimento de alunos, professores ou outros elementos da comunidade educativa, o endereço será comunicado ao Coordenador de Segurança Digital que, por sua vez, documentará o incidente e fá-lo-á chegar ao Órgão de Gestão, conforme adequado.
- Qualquer material que a escola considere ser ilegal será denunciado através dos mecanismos oficiais, segundo as normas em vigor.
- A escola toma todas as precauções possíveis para garantir que os utilizadores acedam apenas a conteúdo digital apropriado. No entanto, devido à natureza global e diversidade disponível nas redes, para além do fato de os alunos poderem utilizar equipamento pessoal, nem sempre é possível evitar, atempadamente, o uso indevido.
- Todos os membros da comunidade escolar que violarem os sistemas de filtragem ou

acederem a sítios com conteúdos inadequados ao espaço escolar serão alvo de procedimento disciplinar, de acordo com o RI.

- São feitas verificações semestrais, ou sempre que detetada alguma anomalia, para comprovar a eficácia dos métodos de filtragem adotados.

6. Decisões quanto às políticas

6.1. Autorização do acesso à Internet

- O AEDCPF manterá um registo atualizado de todos os alunos e professores que são autorizados a aceder às comunicações eletrónicas da escola.
- Todos os elementos da comunidade terão conhecimento da Política de Segurança Digital e dos recursos para a utilização segura da Internet, disponíveis no sítio Web do AEDCPF e serão incentivados a analisá-los com os seus educados.

6.2. Resolução de incidentes relativos à Segurança Digital

- Todos os elementos da comunidade escolar deverão informar o Coordenador da Segurança Digital caso tenham conhecimento de situações preocupantes, do ponto de vista da segurança digital (tais como violações do sistema de filtragem, ciberbullying, conteúdos ilícitos, utilização inadequada de equipamento, etc.).
- As queixas relativas à utilização indevida da Internet serão tratadas no quadro dos procedimentos de apresentação de queixas ou denúncias adotadas pela escola.
- 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 AEDCPF contactará a Equipa de Proteção de Menores, através da Direção e / ou Coordenador da Segurança Digital, encaminhando a situação para as autoridades competentes.

6.3. Gestão dos casos de ciberbullying

- O ciberbullying (assim como todas as outras formas de bullying) não será tolerado e todos os incidentes detetados serão comunicados à Direção e / ou Coordenador da Segurança Digital e às autoridades competentes, quando necessário.
- Alunos, professores e pais/encarregados de educação serão aconselhados a manter um registo como prova.
- Serão adotados procedimentos claros para investigar incidentes ou alegados casos de ciberbullying.
- Será solicitado a alunos, professores e pais/encarregados de educação que trabalhem em conjunto com a escola, de modo a apoiarem a abordagem da escola em relação ao ciberbullying e à segurança digital.
- Todos os elementos da escola serão sensibilizados para a importância de manterem uma conduta adequada na Internet e de não publicarem comentários, conteúdos, imagens ou vídeos na Internet que possam causar dano, prejuízo ou sofrimento a outros elementos da comunidade escolar.

- As sanções para os envolvidos em ciberbullying podem incluir:
  - A eliminação de todo o material considerado inapropriado pelo(a) autor(a) dos atos ou, caso se recuse ou não seja capaz de o fazer, eliminação realizada pelo fornecedor do serviço para que apague os conteúdos em questão;
  - A implementação de sanções, devidamente informada aos pais / encarregados de educação;
  - O contato e denúncia às autoridades judiciais, caso se suspeite de ação ilícita.
- Gestão de telemóveis e equipamentos pessoais.
- Os telemóveis ou equipamentos pessoais não podem ser utilizados durante as aulas ou tempos letivos formais (devendo, por isso, estar desligados), a não ser para efeitos pedagógicos devidamente autorizados, orientados e supervisionados pelo professor.
- Os utilizadores são responsáveis por qualquer tipo de dispositivos eletrónicos que tragam para a escola. A escola 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.
- 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.
- Os professores ou outros responsáveis podem confiscar um telemóvel ou outros equipamentos eletrónicos, conforme o estabelecido no Regulamento Interno, se suspeitar que o equipamento pessoal contém materiais que podem constituir prova de uma ação ilícita.
- No caso de apreensão, cumprir-se-á o estipulado no Regulamento Interno.
- 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.
- Se um(a) aluno(a) necessitar de contactar os pais ou encarregado de educação, deve usar, preferencialmente, o telefone da escola ou contactar os pais ou encarregado de educação através do seu telemóvel, em período não letivo e fora de espaços como salas de aula, biblioteca, zonas comuns dos blocos e outros espaços onde possa perturbar o funcionamento dos serviços.
- Os pais e encarregados de educação não devem contatar os filhos/educandos para os telemóveis durante o horário letivo. Em caso de necessidade de contato urgente devem usar o número de telefone da Escola.
- Os professores e educadores não devem preferencialmente utilizar os seus telemóveis ou equipamentos pessoais para contactar crianças ou jovens dentro ou fora da escola na sua qualidade de profissionais, a não ser em situações de emergência e quando outros meios de contato não estejam operacionais.
- Sempre que for necessário contactar alunos ou pais/encarregados de educação, deverão usar um telefone da escola.
- A captura de imagem e / ou vídeo deverá ser feita com equipamentos disponíveis no AEDCPF.
- Se um docente violar as políticas da escola, podem ser tomadas medidas disciplinares.

7. Conhecimento das políticas

7.1. Conhecimento das políticas pelo pessoal docente, não docente e pais e encarregados de educação

- A Política de Segurança Digital está disponível, para conhecimento e consulta, no sítio Web do AEDCPF.
- O AEDCPF ministrará, a todos os elementos da escola, formação atualizada e adequada sobre a utilização segura e responsável da Internet, tanto ao nível profissional como pessoal.
- No sítio Web do AEDCPF são disponibilizados recursos de apoio para uma utilização segura e responsável da Internet e de equipamentos informáticos.