Boas Práticas de Segurança Digital

Este documento tem como objetivo promover a utilização saudável, responsável e segura da Internet, das plataformas e ferramentas de trabalho utilizadas no agrupamento. Tem também como objetivo sensibilizar, através de um conjunto de boas práticas, a comunidade educativa para a cibersegurança no dia a dia.

Regras Gerais de Cibersegurança

- Ao partilhar qualquer tipo de conteúdo na Internet, deve fazê-lo com cuidado e de forma refletida, pois uma vez colocado na rede, o conteúdo poderá estar disponível para pessoas que não conhece.
- Não deve publicar informações relacionadas com outros utilizadores, sem autorização dos mesmos.
- Não deve responder a ameaças, provocações e intimidações e caso se registem situações deste género, deve reportar imediatamente.
- Deve ocultar os seus dados pessoais, como por exemplo, não divulgar o nome completo, o número do cartão de cidadão, a morada, data de aniversário e/ou outros elementos que possam identificá-lo.
- Deve tornar o perfil das redes sociais privado, para que apenas os seus contactos conhecidos e aprovados possam ver as suas partilhas.
- Não deve reencaminhar e-mails se não estiver seguro do seu conteúdo e deve ocultar os remetentes e/ou outras informações que não sejam necessárias.
- Não deve abrir e-mails suspeitos nem aceder a links que não ofereçam segurança.
- Deve consultar conteúdos web em modo privado ou confidencial para efetuar uma navegação mais segura.
- Não deve copiar conteúdos e deve respeitar os direitos de autor e a propriedade intelectual.
- Deve proteger os seus dispositivos pessoais com pin e/ou palavra-passe, evitando que as mensagens, fotografias e documentos pessoais sejam lidos por pessoas indesejadas, garantindo o direito à individualidade.
- Deve mudar as palavras-passe com regularidade, fazendo cumprir os requisitos mínimos de segurança (no mínimo 8 carateres, utilizar carateres especiais, letras maiúsculas e minúsculas).
- Não deve partilhar palavras-passe.
- Deve verificar sempre se o software dos seus dispositivos está atualizado, em especial, o antivírus.
- Deve ter atenção aos programas e aplicações que se instalam via online, devendo preferencialmente, fazer download de páginas oficiais.
- Deve ter atenção às permissões dadas na instalação de software e/ou aplicações.
- Deve verificar, se na página web que está a utilizar, aparece o “https://” e não “http://”. Se aparecer um cadeado na barra onde se está a navegar, significa que se encontra numa página segura.
- Não deve aceder a pontos wi-fi públicos, mas se aceder, não manipule dados sensíveis.
- Deve fazer cópias de segurança dos seus ficheiros de forma regular.

A Equipa E-Safety,