COLÉGIO DO SAGRADO CORAÇÃO DE MARIA LISBOA

Política de Segurança Digital

ÍNDICE

1. APROVAÇÃO DO DOCUMENTO

	Função	Nome	Razão para a nova versão
Responsável pelo documento	Direção – Coordenadora do JI/PE e Segurança Digital	**Catarina André**	V02 Atualização face ao Regulamento Geral da Proteção de Dados
Consultores	Serviço Técnico de Informática	**José Sebastião Feio**	
	Docentes de TIC	**Carla Soares**	
		Paulo Tavares	
Aprovação	Diretora Pedagógica	Margarida Marrucho Mota Amador	
Data de Aprovação	Reunião de Conselho Pedagógico de 15.05.2018		
Periodicidade de Revisão	Anual	**Próxima revisão**: 2019	
Divulgação	A todos os colaboradores		

A nossa Política de Segurança Digital foi redigida pelo Colégio, tendo como base a Política do Selo de Segurança Digital bem como a norma internacional ISO:9001.

2. MOTIVAÇÃO

O acesso à *Internet*, no espaço escolar, é cada vez mais fácil, pois as tecnologias digitais fazem parte do nosso dia a dia. O número de dispositivos com ligação à *Internet* no espaço escolar é cada vez maior. Grande parte dos colaboradores traz o seu próprio equipamento para o Colégio e usa-o para fins profissionais (*tablets*, computadores portáteis, telemóveis). Estes equipamentos permitem que os docentes, por exemplo, possam alterar dados sensíveis do sistema como as notas, sumários, faltas e tenham acesso aos dados pessoais de alunos e das suas famílias. Por outro lado, é também cada vez maior o número de alunos que trazem dispositivos que permitem ligação à *Internet.*

Para tirar o máximo partido das oportunidades que as tecnologias digitais oferecem é necessário conhecê-las e saber utilizá-las corretamente. Ao adotar políticas de Colégio para a segurança digital podemos garantir um ambiente mais seguro para pais/alunos e colaboradores protegendo e preparando-os para os perigos que uma utilização incorreta pode acarretar.

3. PROCESSO ENSINO E APRENDIZAGEM

3.1. Por que razão é a utilização da *Internet* tão importante?

Discussão:

A rapidez com que evoluem as comunicações eletrónicas afeta a sociedade de várias formas. É importante reafirmar o que pretendemos conseguir na educação por meio da utilização das tecnologias informáticas e da *Internet*.

Declarações: Como serão tratadas as denúncias relacionadas com a segurança digital?

- A utilização da *Internet* fará parte integrante do currículo e é uma ferramenta essencial na aprendizagem.
- A *Internet* faz parte do dia a dia no ensino, nas empresas e na interação social.
- Os alunos utilizam a *Internet* amplamente fora do Colégio e devem saber como avaliar a informação que obtêm e como se podem proteger.
- A finalidade da utilização da *Internet* nas escolas é elevar os padrões educativos, promover o sucesso dos alunos, apoiar o trabalho dos docentes e reforçar a administração escolar.
- O acesso à *Internet* é disponibilizado aos alunos que têm o dever de a utilizar com responsabilidade.

3.2. Quais são os benefícios da utilização da *Internet* no ensino?

Discussão:

Vários estudos salientam os benefícios pedagógicos[1] e educativos que se podem retirar de uma utilização adequada da *Internet*, nomeadamente melhores resultados dos alunos.

Declarações:

- Acesso a recursos pedagógicos e educativos de todo o mundo, incluindo museus e galerias de arte.
- Intercâmbio cultural e educativo entre alunos de vários países.
- Utilização social, recreativa e de lazer nas bibliotecas, nos clubes e em casa.
- Acesso de alunos e docentes a peritos em inúmeras áreas.
- Desenvolvimento profissional dos docentes através do acesso a desenvolvimentos nacionais, materiais pedagógicos e aplicações eficazes do currículo.
- Colaboração no âmbito de redes de escolas, serviços de apoio e associações profissionais.

1 Bellanca J. e Brandt R. (2010). *21st Century Skills: Rethinking How Students Learn*. Solution Tree | Press
Trilling B. e Fadel C. (2009). *21st Century Skills: Learning for life in our times*. 1.ª Edição, Jossey-Bass, San Francisco
P21 Partnership for 21st century learning. Consultado em: 23 de Julho de 2015. No site: http://www.p21.org/

- Maior acesso a apoio técnico, designadamente gestão remota de redes e atualizações automáticas de programas.
- Possibilidade de aprendizagem quando e onde for mais conveniente.

3.3. De que formas pode a utilização da *Internet* melhorar a aprendizagem?

Discussão:

Não basta haver mais computadores disponíveis e um acesso mais facilitado à *Internet*. O impacto nos resultados de aprendizagem dos alunos também deve ser tido em consideração. É essencial desenvolver práticas eficazes de utilização da *Internet* para fins de ensino e aprendizagem. Os alunos necessitam de adquirir capacidades de literacia digital e amadurecer as suas próprias publicações e a comunicação que mantêm com outros através da *Internet*. O respeito pelos direitos de autor e os direitos de propriedade intelectual e a correta utilização de material publicado devem ser ensinados. Devem ainda ser desenvolvidos conhecimentos nos alunos que permitam a estes utilizar recursos disponibilizados na *Internet* através de licenças abertas (i.e. *Creative Commons*). Devem ainda ser adotados métodos de deteção de plágio.

Declarações:

- O acesso à *Internet* no Colégio será pensado com vista a alargar e reforçar a educação.
- Ensinar-se-á 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*.
- Os alunos aprenderão a utilizar eficazmente a *Internet* para fins de pesquisa, designadamente desenvolver competências de procura, obtenção e avaliação de informações.
- 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.
- Os docentes devem indicar as fontes das informações utilizadas e respeitar os direitos de autor quando utilizam material obtido na *Internet* no desenvolvimento das suas funções.

3.4. Como podem os alunos aprender a avaliar conteúdos digitais?

Discussão:

A qualidade da informação recebida através da rádio, dos jornais e do telefone é variável e todos devem desenvolver um sentido crítico na seleção e avaliação da informação. A informação obtida através da *Internet*, de *e-mails* ou de mensagens de texto obriga a cuidados acrescidos no tratamento da informação e a capacidades de literacia digital mais apuradas. Em especial, pode ser difícil determinar a sua origem, intenção e correção, uma vez que o contexto pode estar omisso ou ser de difícil interpretação.

Declarações:

- 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.
- Devem-se mostrar ferramentas de pesquisa da *Internet* que sejam adequadas à idade dos alunos.
- A avaliação de materiais da *Internet* faz parte do processo de ensino e de aprendizagem de qualquer disciplina e será considerada um requisito transversal ao Colégio e ao currículo.
- A configuração de um motor de pesquisa por defeito nos navegadores de *Internet*, com navegação privada, como por exemplo, a disponibilizada através do endereço https://startpage.com, é aconselhada.

4. GESTÃO DE SISTEMAS DE INFORMAÇÃO

4.1. Como é mantida a segurança dos sistemas de informação?

Discussão:

É importante rever a segurança de todo o sistema, desde os utilizadores até à *Internet*. Esta é uma questão de extrema responsabilidade que abrange, não só o fornecimento de serviços de aprendizagem essenciais, mas também a própria segurança pessoal de alunos, colaboradores, encarregados de educação e outros.

Declarações:

- A segurança dos sistemas informáticos do Colégio e dos utilizadores será revista com regularidade.
- A proteção antivírus será atualizada com regularidade.
- As regras do *firewall* devem ser conhecidas e atualizadas de acordo com as ameaças de cybersegurança.
- Os dados pessoais enviados através da *Internet* ou transferidos para fora do Colégio serão encriptados.
- *Software* não aprovado não será autorizado nas áreas de trabalho ou como anexo de mensagens eletrónicas.
- Os ficheiros guardados na rede do Colégio serão verificados com regularidade.
- O coordenador do Serviço Técnico de Informática analisará a capacidade e o funcionamento do sistema com regularidade.
- A utilização de nomes de utilizador e palavras-passe para aceder à rede do Colégio deverá ser obrigatória.
- A integração de extensões de programas nos navegadores de *Internet*, tais como o *disconnect.me* , *Adblock plus*, *Ghostery* ou outros semelhantes, poderá permitir a utilização

de uma navegação mais privada e com menor índice de publicidade não desejada, durante o uso da *web*.

4.2. Como será feita a gestão do correio eletrónico?

Discussão:

O correio eletrónico (*e-mail*) é um meio de comunicação essencial para alunos e colaboradores do Colégio. Uma utilização bem regulada do *e-mail* permite obter grandes benefícios pedagógicos e administrativos. É possível, por exemplo, desenvolver projetos interessantes entre escolas de localidades vizinhas ou mesmo de outros continentes.

A não regulação do *e-mail* pode abrir caminhos aos alunos que contornam os limites tradicionais do Colégio. É possível a restrição do envio e receção de mensagens a endereços de *e-mail* aprovados e a filtragem de conteúdos não adequados.
No contexto escolar, o *e-mail* não deve ser considerado privado e a maioria das escolas reserva-se o direito de monitorizá-lo, assegurando o sigilo profissional e com o conhecimento do próprio. Há que encontrar um equilíbrio adequado entre a necessidade de monitorização para assegurar a segurança de alunos e colaboradores, por um lado, e a preservação dos direitos humanos, por outro, ambos previstos em legislação recente.

É fundamental que o colaborador compreenda que deve utilizar uma conta de *e-mail* fornecida pelo Colégio para comunicar com pais/encarregados de educação, alunos e outros profissionais sobre assuntos oficiais e relacionados com o Colégio. Este facto é importante por razões de confidencialidade e segurança, assim como para proteger os elementos do Colégio de eventuais acusações ou ações.

O e-mail é um potencial ponto de entrada de *malware*, através do envio de mensagens com vírus, *trojans* ou *phishing*.

Declarações:

- Os alunos apenas podem utilizar contas de *e-mail* aprovadas para assuntos relacionados com o Colégio.
- Os alunos têm de informar imediatamente o colaborador designado para o efeito caso recebam mensagens de *e-mail* ofensivas.
- Os alunos não podem revelar dados pessoais sobre eles próprios ou outros numa mensagem eletrónica, nem combinar encontrar-se com alguém sem autorização expressa

de um adulto.

- Os colaboradores do Colégio devem utilizar os endereços fornecidos pelo Colégio apenas para comunicar com alunos e pais/encarregados de educação, conforme aprovado pela equipa de apoio à Direção.
- As mensagens de *e-mail* enviadas para organizações externas devem ser escritas cuidadosamente antes de serem enviadas, do mesmo modo que o seria uma carta enviada em papel timbrado do Colégio.
- O reencaminhamento de mensagens em cadeia não é autorizado.
- O colaborador deve zelar pela segurança do sistema.
    - O Serviço Técnico de Informática não enviará e-mails a pedir a confirmação de identidade ou a validação do acesso ao sistema.
    - Não deve seguir *links*, sem avaliar cuidadosamente a sua proveniência.
    - Não deve introduzir o utilizador e senha de acesso, sem verificar que o serviço que está a aceder pertence ao domínio do Colégio – CSCM-LX.PT.

4.3. Como será feita a gestão dos conteúdos publicados?

Discussão:

Muitas escolas criaram sítios na *Internet* e outros canais de comunicação de excelente qualidade que inspiram os alunos a publicar trabalhos de alto nível. Os sítios na Rede divulgam o trabalho dos alunos, promovem o Colégio e publicam recursos para a realização de projetos.

Assegurar orientações de caráter editorial ajudará o Colégio a espelhar os requisitos de correção linguística e boa apresentação.

Declarações:

- As informações de contacto no sítio na Rede devem ser a morada, o número de telefone e o *e-mail* do Colégio. Não deve ser publicada qualquer informação pessoal de alunos ou colaboradores.
- A Diretora Pedagógica é a responsável editorial geral pelos conteúdos digitais publicados pelo Colégio na *Internet* e deve assegurar que os conteúdos publicados são corretos e adequados.
- O sítio do Colégio na Rede deve cumprir as diretrizes do Colégio em matéria de publicações, designadamente, respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

4.4 Podem publicar-se fotografias e trabalhos de alunos?

Discussão:

Fotografias e registos vídeo e áudio criam dinamismo e interesse numa publicação, especialmente se incluírem alunos. No entanto, a segurança de alunos e restantes elementos do Colégio é primordial.

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. Os alunos que figurem nas fotografias devem, naturalmente, estar vestidos de forma adequada.

O Colégio solicita autorização para publicar imagens de trabalhos ou fotografias pessoais adequadas quando o aluno se matricula ou uma vez em cada ano letivo.

Cabe também aos alunos aprender as razões pelas quais devem ter cuidado ao publicar informações e imagens pessoais *online*.

Declarações:

- As imagens ou gravações vídeo que incluem alunos serão selecionadas cuidadosamente.
- Os nomes completos dos alunos não serão utilizados em parte alguma do *site* do Colégio da rede, em especial junto a fotografias.
- O Colégio tem o direito de publicar fotografias individualizadas de alunos, à exceção de grandes planos. Esta indicação carece de autorização expressa do Encarregado de Educação.
- O consentimento por escrito será mantido pelo Colégio sempre que as imagens de alunos forem utilizadas para fins publicitários externos ao Colégio e até as imagens em causa deixarem de ser usadas.
- Os trabalhos produzidos pelos alunos são propriedade do próprio. Contudo, o Colégio poderá publicá-los identificando o respetivo autor.

4.5. Como será feita a gestão de comunidades sociais virtuais, redes sociais e publicações pessoais?

Discussão:

Os pais/encarregados de educação e os docentes devem estar cientes de que a *Internet* tem

espaços virtuais e redes sociais a aparecer constantemente que permitem às pessoas publicar conteúdos sem qualquer mediação. Os sítios das redes sociais permitem que pessoas com interesses semelhantes ou totalmente diversos estejam ligadas entre si. Os utilizadores são frequentemente convidados a aceder a espaços pessoais e a publicar comentários, sobre os quais existe um controlo bastante limitado.

Para os adultos responsáveis, os sítios das redes sociais permitem o acesso fácil e gratuito a várias funcionalidades, embora por vezes a publicidade seja invasiva e alguns sítios possam ser de conteúdo duvidoso. Os alunos devem ser encorajados a refletir sobre a facilidade com que se publica informação pessoal, os perigos associados e a dificuldade (impossibilidade em alguns casos) em eliminar uma imagem ou informação menos própria depois de esta ter sido publicada.

Os docentes devem ser alertados para os potenciais riscos subjacentes à utilização de redes sociais ou à publicação de informações pessoais, seja profissionalmente com os alunos ou a título pessoal. Devem ser alertados para a importância de selecionar o material que publicam, de verificar a segurança dos perfis e a forma como a publicação de materiais inadequados pode afetar o seu estatuto profissional. São exemplos de redes sociais e ferramentas de publicação: blogues, *wikis*, comunidades virtuais, fóruns, jogos *online* com vários jogadores, salas de conversação, sistemas de mensagens instantâneas, entre muitos outros.

Declarações:

- O Colégio poderá controlar o acesso a comunidades virtuais e a redes sociais.
- Os alunos serão aconselhados a nunca fornecerem quaisquer dados de caráter pessoal que permitam identificá-los e/ou o local onde se encontram, por exemplo, o seu nome verdadeiro, a morada, o número de telefone ou telemóvel, o Colégio que frequentam, endereços de *e-mail* ou de sistemas de mensagens instantâneas, nomes completos de amigos/familiares, interesses específicos, clubes, etc.
- Os docentes 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.
- Os blogues ou *wikis* oficiais geridos pelos docentes devem estar protegidos por palavra-passe e ser executados a partir do sítio na Rede do Colégio com a aprovação da equipa de apoio à Direção. Recomendar-se-á que os docentes não criem espaços em redes sociais que destinem a ser usados pelos alunos numa base pessoal.
- Os alunos serão aconselhados quanto a questões de segurança e privacidade na *Internet* e incentivados a definir palavras-passe, negar o acesso a desconhecidos e bloquear comunicações não desejadas. Os alunos serão incentivados a aceitar e convidar apenas

amigos conhecidos em sítios de redes sociais e a negar o acesso a outros, tornando para tal, o seu perfil privado.

- Todos os elementos da comunidade escolar são aconselhados a não publicar opiniões pessoais específicas e pormenorizadas, especialmente se estas puderem ser consideradas ameaçadoras, ofensivas ou difamatórias.
- Serão abordadas com os pais/encarregados de educação questões e preocupações relacionadas com a utilização de redes sociais, meios sociais e sítios de publicação pessoal (dentro ou fora do Colégio), especialmente quando se trata de alunos mais novos.
- A utilização pessoal por parte dos elementos do Colégio de comunidades virtuais, redes sociais, meios sociais e sítios de publicação pessoal será discutido enquanto parte da formação inicial no local de trabalho e nas Políticas de Utilização Aceitável serão definidas as condutas consideradas seguras e profissionais.

4.6. Como será feita a gestão dos sistemas de filtragem?

Discussão:
Os níveis de acesso à *Internet* e de supervisão serão variáveis em função da idade e da experiência dos alunos. Os perfis de acesso devem estar adequados a todos os elementos da comunidade escolar. No âmbito de projetos supervisionados por docentes, os alunos mais velhos poderão necessitar de aceder a determinados materiais com conteúdos para adultos; por exemplo, para redigir um texto ou encenar uma peça de teatro poderão necessitar de incluir referências à sexualidade. Os docentes, por seu turno, poderão necessitar de pesquisar assuntos como drogas, problemas de saúde, *bullying*, racismo ou assédio sexual. Nestes casos, o uso é legítimo, pelo que deve ser aprovado e quaisquer restrições deverão ser retiradas temporariamente. Existem sistemas que permitem adaptar o perfil de acesso à idade e maturidade dos alunos.

Os controlos de acesso estão categorizados em várias tipologias, que se sobrepõem (habitualmente conhecidos como filtros):

- Estratégias de bloqueio impedem o acesso a uma lista de sítios indesejáveis. A manutenção da lista de sítios bloqueados não é uma tarefa fácil na medida em que todos os dias surgem novos sítios na *Internet*.
- O chamado "jardim murado" ou "lista de aprovados" limita o acesso apenas à lista de sítios aprovados. Tais listas confinam inevitavelmente o acesso dos alunos a um leque restrito de

conteúdos.

- Uma filtragem dinâmica de conteúdos analisa o conteúdo dos sítios na *Internet* ou dos *e-mails* com base em palavras inadequadas.
- As listas de palavras-chave filtram as pesquisas nos motores de busca e nos endereços à procura de resultados e endereços *web* inadequados. Os sistemas baseados em classificações atribuem uma classificação a cada sítio na *Internet* em função do seu conteúdo sexual, profano, violento ou inadequado por outros motivos. Os programas de navegação na *Internet* podem ser configurados para rejeitar sítios com uma classificação que ultrapasse um determinado limiar.
- Os sistemas de registo de endereços permitem monitorizar os sítios na *Internet* visitados pelos utilizadores individualmente. Podem criar-se relatórios que permitam investigar o acesso dos alunos.
- Os registos de teclado registam todo o texto enviado por um computador e fazem uma análise de padrões.

Ocasionalmente, podem ocorrer erros e é possível aceder a conteúdos não adequados, ou outros que são adequados e que são bloqueados. Por conseguinte, é importante que as crianças estejam sempre sob supervisão quando acedem à *Internet* e que as Políticas de Utilização Aceitável sejam cumpridas.
Qualquer material que o Colégio considere ser ilegal, de acordo com a legislação portuguesa, deve ser denunciado à linha nacional.

Declarações:

- O acesso à *Internet* fornecido pelo Colégio incluirá sistemas de filtragem adequados à idade e à maturidade dos alunos.
- O Colégio colocará em prática procedimentos claros para denunciar violações do sistema de filtragem. Todos os elementos do Colégio, colaboradores, alunos e pais/encarregados de educação devem ter conhecimento destes procedimentos.
- Se sítios indesejáveis chegarem ao conhecimento de alunos e colaboradores, o endereço será comunicado ao Coordenador de Segurança Digital do Colégio, que, por sua vez, documentará o incidente e fá-lo-á chegar à pessoa responsável, conforme adequado.
- Quaisquer alterações ao sistema de filtragem do Colégio serão avaliadas, em função do risco, por membros da equipa com experiência pedagógica e técnica antes de serem postas em prática e, sempre que adequado, com o consentimento da equipa de apoio à Direção.
- A equipa de apoio à Direção deve assegurar que são feitas verificações regulares para

comprovar a eficácia dos métodos de filtragem adotados.

- A estratégia de acesso à *Internet* do Colégio deve ser delineada por educadores, com o apoio dos gestores da rede, de forma a estar em consonância com a idade e o currículo dos alunos.

4.7 Como são geridas as tecnologias emergentes?

Discussão:

Muitas tecnologias de comunicação emergentes, como as comunicações móveis, o acesso à *Internet* e as ferramentas colaborativas e multimédia, possuem um enorme potencial de desenvolvimento de novas ferramentas de ensino e aprendizagem. Para cada nova tecnologia, deve ser realizada uma avaliação dos riscos com vista a desenvolver práticas eficazes e seguras de utilização em sala de aula. A abordagem mais segura é negar o acesso até à conclusão da avaliação de riscos e à confirmação de segurança, no entanto não é a mais aconselhada do ponto de vista do desenvolvimento pessoal e social dos alunos e crianças.

As comunidades e salas de aula virtuais alargam os limites geográficos da aprendizagem. Abordagens como o *mentoring*, a aprendizagem a distância e o acesso parental fazem cada vez mais parte dos sistemas escolares. As comunidades virtuais podem igualmente ser uma forma de incentivar alunos desmotivados a serem mais participativos.

A segurança e a eficácia das comunidades virtuais dependem dos seus utilizadores serem, eles próprios, identificáveis e dignos de confiança, o que nem sempre é fácil, visto a autenticação fora do Colégio ser difícil, como é claramente comprovado por sítios de redes sociais e outras ferramentas digitais como o *Facebook*, o *YouTube*, o *Skype* e o *Twitter*, entre outras. O registo pessoal, com o intuito de se estabelecer e manter identidades eletrónicas validadas, é essencial para uma comunicação segura, mas nem sempre é possível.

A videoconferência possibilita novas dimensões. As *webcams* são cada vez mais baratas e, com acessos à *Internet* cada vez mais rápidos, permitem a partilha de vídeos através da *Internet*. A disponibilidade de ligações vídeo em tempo real pode por vezes aumentar a segurança - podemos ver com quem estamos a falar – mas, se utilizada indevidamente, uma ligação vídeo pode revelar dados de segurança.

Novas aplicações estão continuamente a ser desenvolvidas com base na *Internet*, nos telemóveis, nas redes sem fios, nas ligações por *bluetooth* ou infravermelhos. Quando usam o telefone, as consolas de jogos ou os dispositivos móveis com acesso sem fios à *Internet*, os utilizadores já não precisam de estar fixos. Esta mobilidade oferece não só infinitas oportunidades de aprendizagem, mas também tem riscos, como quando um aluno grava a reação de um colaborador numa situação difícil.

As escolas devem manter-se atualizadas no que respeita às novas tecnologias, nomeadamente, as relacionadas com telemóveis e dispositivos móveis, e estar prontas a definir estratégias adequadas. Por exemplo, o envio de mensagens instantâneas através dos telemóveis é uma atividade frequente para muitos alunos e famílias e é um meio que pode ser utilizado para comunicar uma ausência do aluno ou para enviar lembretes de exames ou trabalhos. Naturalmente que o uso dos telemóveis pessoais acarreta riscos para os colaboradores, no caso de serem usados para contactar os alunos, pelo que devem ser previstos telemóveis do Colégio para o efeito e definir uma política de uso específico deste tipo de dispositivos regulado através do Regulamento Interno.

A inclusão de linguagem ou de imagens inapropriadas é difícil de detetar pelos colaboradores. Poderá ser necessário relembrar os alunos que tal utilização não é adequada e é contrária às políticas do Colégio. As mensagens abusivas devem ser tratadas de acordo com as políticas de conduta e/ou *anti-bullying* do Colégio.

Declarações:

- As tecnologias emergentes serão avaliadas em termos de benefícios pedagógicos, devendo ser realizada uma análise de riscos antes de a sua utilização no Colégio ser autorizada.
- Os alunos deverão ser instruídos sobre a utilização adequada e segura de equipamentos pessoais dentro e fora do Colégio em conformidade com a política do Colégio em matéria de utilização de telemóveis (Regulamento Interno) e as Políticas de Utilização Aceitável .

5. DECISÕES QUANTO ÀS POLÍTICAS

5.1. Como será autorizado o acesso à *Internet*?

Discussão:

O Colégio deve autorizar o acesso à *Internet* a alunos e colaboradores com base em necessidades pedagógicas e administrativas.

Declarações:

- Entende-se por *Internet* as redes de dados locais, por cabo ou *wireless* (sem fios), bem como as redes externas ao Colégio, fornecidas por um provedor de serviço.
- O acesso à *Internet* é facultado a toda a comunidade educativa podendo ser alvo de monitorização e gravação.
- Os utilizadores regulares (colaboradores, alunos e pais/encarregados de educação) têm acesso à rede *wireless* após autenticação com o seu utilizador e senha pessoais.
- Os utilizadores não regulares têm acesso à rede *wireless* após a atribuição de uma

credencial temporária, criada para o efeito.

5.2. Como deve o Colégio reagir a incidentes preocupantes?

Discussão:

A *Internet* e as comunicações eletrónicas oferecem a crianças e jovens oportunidades extraordinárias de alargarem as suas experiências de aprendizagem e desenvolverem a sua criatividade dentro e fora do Colégio. No entanto, é igualmente importante considerar os riscos associados à forma como estas tecnologias podem ser utilizadas. Uma Política de Segurança Digital deve reconhecer e procurar desenvolver as competências de que as crianças e os jovens necessitam quando comunicam e usam tecnologias a fim de se manterem seguros e agirem com respeito para com os outros.

As pessoas que atuam de forma desadequada ou ilegal podem ser confrontadas com riscos de segurança digital, seja sem intenção, seja deliberadamente.

Todas as situações que suscitem preocupação devem ser tratadas de modo pessoal.

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

Os restantes colaboradores do Colégio também devem contribuir para o desenvolvimento de uma cultura de segurança, estando atentos aos comportamentos uns dos outros na *Internet* e falando sobre eventuais problemas. Qualquer atividade ilegal deve ser reportada ao Coordenador de Segurança Digital do Colégio.

Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal que envolva a utilização de equipamento informático, as escolas devem determinar o nível de resposta adequado à infração em questão. Caso se considere que a infração ultrapassa o âmbito de responsabilidades do Colégio, a decisão de recorrer à intervenção das autoridades deve ser tomada, o mais cedo possível, pela Direção do Colégio.

Declarações:

- Todos os elementos do Colégio 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).
- O Coordenador de Segurança Digital registará todos os incidentes comunicados e todas as medidas tomadas no registo de incidentes relacionados com a segurança digital.
- O Colégio gerirá os incidentes relacionados com a segurança digital em conformidade com o Regulamento Interno.
- O Colégio informará os pais/encarregados de educação sobre quaisquer incidentes ou preocupações, quando e como considerar mais adequado.

- Depois de concluídas eventuais investigações, o Colégio fará o ponto da situação, retirará ilações do ocorrido e, se necessário, tomará medidas.
- Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal, o Colégio contactará a Equipa de Proteção de Menores, o/a responsável pelas questões de segurança digital ou outra pessoa competente e encaminhará a situação para a Polícia.

5.3. Como serão tratadas as denúncias relacionadas com a segurança digital?

Discussão:

Pais/encarregados de educação, colaboradores e alunos devem saber qual o procedimento que o Colégio adotou para apresentar uma denúncia. Os factos do incidente ou da preocupação devem ser estabelecidos e devem reunir-se todas as provas sempre que possível e adequado. Os incidentes relacionados com a segurança digital podem afetar alunos, colaboradores e a comunidade escolar alargada, tanto dentro como fora do Colégio, e podem ter consequências ao nível civil, legal e disciplinar.

Uma transgressão menor das regras pode ser tratada por um elemento do Colégio. Outras situações potencialmente graves podem exigir vários tipos de sanções que devem estar ligadas ao Regulamento Interno. Situações ilícitas ou eventualmente relacionadas com a proteção de menores devem ser remetidas às autoridades responsáveis.

Declarações:

- As ocorrências relativas à utilização indevida da *Internet* serão tratadas no quadro dos procedimentos de apresentação de queixas ou denúncias adotado pelo Colégio.
- Quaisquer ocorrências que envolvam a utilização indevida da *Internet* por pessoal docente ou não docente serão encaminhadas para a Diretora.
- O Colégio manterá um registo de todos os incidentes ou queixas relacionados com a segurança digital, assim como das medidas tomadas.
- Os colaboradores, os alunos e os pais/encarregados de educação serão informados dos procedimentos necessários para apresentação de ocorrências.
- Os colaboradores, os alunos e os pais/encarregados de educação trabalharão em conjunto com o Colégio com vista à resolução dos problemas.
- Todos os elementos do Colégio necessitam de compreender a importância da confidencialidade e a necessidade de seguir os procedimentos oficiais do Colégio para comunicação de situações preocupantes.
- Quaisquer situações (incluindo sanções) serão tratadas de acordo com o Regulamento

Interno do Colégio.

- Todos os elementos do Colégio 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.

5.4. Como serão geridos os casos de *cyberbullying*?

Discussão:

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".

Para muitos jovens e adultos, a *Internet* e os telemóveis constituem uma parte criativa e positiva da sua vida quotidiana. Infelizmente, as tecnologias também podem ser utilizadas de uma forma negativa. Quando as crianças são alvo de *bullying,* através de telemóveis, jogos ou da *Internet*, podem sentir-se sozinhas, particularmente se os adultos à sua volta não perceberem o *cyberbullying* e os seus efeitos. Um ambiente ou atividade que até então era seguro e divertido torna-se ameaçador e uma fonte de ansiedade e sofrimento.

É essencial que alunos, colaboradores e pais/encarregados de educação compreendam que o *cyberbullying* é diferente de outras formas de *bullying*, pela forma como pode afetar as pessoas. Promover uma cultura de utilizadores confiantes promove a inovação e a segurança.

Declarações:

- O *cyberbullying* (assim como todas as outras formas de *bullying*) gerado por qualquer elemento do Colégio, não será tolerado.
- Existem procedimentos claros adotados pelo Colégio para dar apoio a qualquer elemento da comunidade escolar que seja alvo de *cyberbullying*.
- Todos os incidentes de *cyberbullying* comunicados ao Colégio serão registados.
- Serão adotados procedimentos claros para investigar incidentes ou alegados casos de *cyberbullying*.
- Alunos, colaboradores e pais/encarregados de educação serão aconselhados a manter um registo do *bullying* como prova.
- O Colégio tomará medidas para identificar o/a responsável pela situação de *bullying*, sempre que possível e adequado. Isto poderá passar pela análise dos registos informáticos do Colégio, por identificar e entrevistar possíveis testemunhas e contactar o fornecedor do serviço e a polícia, se necessário.
- Será solicitado a alunos, colaboradores e pais/encarregados de educação que trabalhem

em conjunto com o Colégio de modo a apoiarem a abordagem do Colégio em relação ao *cyberbullying* e à segurança digital.

- As sanções para os envolvidos em *cyberbullying* estão descritas no Regulamento Interno do Colégio.

5.5. Como será feita a gestão de telemóveis e equipamentos pessoais?

Discussão:

Os telemóveis e outros equipamentos pessoais, como sejam consolas de jogos e *tablets* são considerados objetos do dia a dia na sociedade atual e até as crianças mais novas possuem e utilizam equipamentos pessoais para aceder à *Internet* regularmente. Os telemóveis e outros equipamentos com acesso à *Internet* são usados para comunicar de várias formas, sendo o envio de mensagens, as câmaras de telemóveis e o acesso à *Internet* funções muito comuns.

No entanto, os telemóveis podem estar na origem de inúmeros problemas quando não são utilizados adequadamente:

São objetos de valor que podem ser roubados ou danificados.

A sua utilização pode tornar alunos ou colaboradores alvo de *cyberbullying*.

O acesso à *Internet* em telemóveis e outros equipamentos pessoais permite que os alunos contornem os sistemas de filtragem e as configurações de segurança do Colégio.

Podem pôr em causa a disciplina na sala de aula, na medida em que podem ser utilizados em modo de “silêncio”.

Os telemóveis com câmaras integradas podem suscitar problemas relacionados com a proteção de menores, *bullying* e proteção de dados ligados à gravação, uso ou distribuição de imagens de alunos ou colaboradores.

Em virtude da utilização generalizada de equipamentos pessoais, é essencial que o Colégio tome medidas para assegurar que os telemóveis e outros equipamentos são utilizados de forma responsável e que a utilização dos telemóveis pelos alunos não impede o ensino, a aprendizagem e a ordem na sala de aula.

A utilização de telemóveis e outros equipamentos pessoais é uma decisão do Colégio, mas os aspetos seguintes constituem uma ajuda ao Colégio na criação de políticas eficazes.

Declarações:

- A utilização de telemóveis e outros equipamentos pessoais por parte de alunos e colaboradores dentro do Colégio constituirá uma decisão do Colégio e fará parte integrante das Políticas de Utilização Aceitável do Colégio ou das políticas relativas à utilização de telemóveis.
- O envio de mensagens ou conteúdos abusivos ou inadequados através de telemóveis ou equipamentos pessoais por parte de qualquer elemento do Colégio é proibido e quaisquer

violações deste princípio serão tratadas em conformidade com o Regulamento Interno.

- Os colaboradores podem confiscar um telemóvel ou equipamento se considerarem que está a ser utilizado de modo contrário às políticas do Colégio em matéria de conduta ou *bullying*. A equipa de apoio à Direção pode fazer uma pesquisa ao telemóvel ou equipamento com o consentimento do aluno ou dos pais/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.
- Os telemóveis não podem ser utilizados durante as aulas ou tempos letivos formais exceto se fizerem parte de uma atividade curricular aprovada e com o consentimento do docente, englobada na política de uso ou no Regulamento Interno.
- Os utilizadores são responsáveis pelos dispositivos eletrónicos de todos os tipos que tragam para o Colégio. O Colégio 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 do Colégio, como vestiários ou casas de banho.

5.5.1. Utilização de equipamentos pessoais pelos alunos

- Se um aluno violar as políticas do Colégio, o seu telemóvel ou equipamento será apreendido e guardado em local seguro no Colégio. Os telemóveis e outros equipamentos pessoais serão entregues aos pais/encarregados de educação, em conformidade com as políticas do Colégio.
- Não é permitido levar telemóveis e outros equipamentos para os exames. Os alunos que tenham um telemóvel na sua posse durante um exame estarão sujeitos à política do organismo responsável pelo exame, o que poderá resultar na anulação do exame ou na impossibilidade de voltar a apresentar-se a outro exame.
- Se um aluno necessitar de contactar os pais/encarregado de educação, ser-lhe-á facultado um telefone do Colégio. Os pais/encarregado de educação são aconselhados a não contactar os filhos para os telemóveis durante o horário letivo, mas a contactar o Colégio, em vez disso.
- 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.

5.5.2. Utilização de equipamentos pessoais pelos colaboradores

- Sempre que for necessário contactar alunos ou pais/encarregados de educação, deverão usar um telefone do Colégio.
- Os telemóveis e outros equipamentos estarão desligados ou em modo de "silêncio", a comunicação *bluetooth* estará “oculta” ou desligada e os telemóveis e outros equipamentos não serão utilizados em períodos letivos, exceto em situações de emergência autorizadas pela equipa de apoio à Direção.
- Se os docentes pretenderem que os alunos utilizem telemóveis ou outros equipamentos pessoais numa atividade educativa, isso será feito de acordo com a política de Segurança digital.
- Os colaboradores não devem utilizar equipamentos pessoais, como telemóveis ou câmaras, para tirar fotografias ou gravar vídeos dos alunos, exceto em situações, com fins pedagógicos, autorizadas pelo Colégio.
- Todos os documentos de trabalho produzidos por colaboradores nos equipamentos pessoais devem ser eliminados depois de concluídos. A versão final deve ser guardada nas plataformas do Colégio, conforme a sua natureza.
- Se um colaborador violar as políticas do Colégio, podem ser tomadas medidas disciplinares.

6. CONHECIMENTO DAS POLÍTICAS

6.1. Como é que o colaborador tem conhecimento das políticas?

Discussão:

É importante que todos os docentes se sintam confiantes para utilizar as novas tecnologias no ensino, pois a Política de Segurança Digital do Colégio só será eficaz se todos os docentes subscreverem os valores e métodos nela consagrados.

Devem ser dadas oportunidades aos docentes para discutirem essas questões e desenvolver estratégias de ensino adequadas. Poderá ser pouco razoável, por exemplo, pedir a docentes em regime de substituição que assumam a orientação de uma atividade com o uso da *Internet* sem qualquer preparação.

Deve ser dada especial atenção quando o Colégio disponibiliza aos colaboradores equipamentos

que podem ser acedidos fora da rede do Colégio. As escolas devem ser claras quanto à utilização segura e adequada dos equipamentos por ela disponibilizados e devem ter regras sobre o uso de equipamento por terceiros. Os colaboradores devem estar cientes de que são responsáveis por manter a confidencialidade da informação do Colégio.
A utilização das tecnologias de comunicação e informação está generalizada. Todos os elementos do Colégio, devem participar nas ações de formação e sensibilização.

Declarações:

- A Política de Segurança Digital será apresentada formalmente e discutida com todos os elementos do Colégio.
- O Colégio irá implementar Políticas de Utilização Aceitável, com o intuito de proteger alunos, colaboradores e outros elementos.
- Discrição e conduta profissional são essenciais.
- O Colégio ministrará a todos os elementos do Colégio uma formação atualizada e adequada sobre a utilização segura e responsável da *Internet*, tanto ao nível profissional como pessoal.
- Os responsáveis pela gestão dos sistemas de filtragem e pela monitorização do uso das TIC serão supervisionados pela equipa de apoio à Direção e terão procedimentos bem definidos para comunicação de incidentes. A comunicação de incidentes deverá estar enquadrada com a política geral de segurança do Colégio.
- O Colégio manterá os docentes a par de ferramentas digitais úteis que podem usar com os alunos na sala de aula. Estas ferramentas variam em função da idade e das capacidades dos alunos.
- Todos os elementos do Colégio deverão estar cientes de que a sua conduta na *Internet* fora do Colégio pode afetar as suas funções e a sua reputação dentro do Colégio.

6.2. Como se pode obter o apoio dos pais/encarregados de educação?

Discussão:

A utilização da *Internet* em casa pelos alunos está a aumentar rapidamente graças aos baixos custos do acesso e aos avanços nas tecnologias móveis. A não ser que os pais/encarregados de educação estejam conscientes dos riscos, os alunos podem ter acesso livre e sem supervisão à *Internet* nas suas próprias casas. O Colégio pode ajudar os pais/encarregados de educação a

definir uma utilização adequada e supervisionada da *Internet* em casa e ajudá-los a perceber os riscos envolvidos. Os pais/encarregados de educação devem ser aconselhados a averiguar se os seus educandos utilizam a *Internet* noutro local e se esse acesso está coberto por uma política de utilização adequada.

Uma estratégia possível é ajudar os pais/encarregados de educação a saber mais sobre as novas tecnologias, por exemplo, através de ações de formação e sessões de sensibilização para os pais/encarregados de educação.

Declarações:

- O Colégio publicará a sua Política de Segurança Digital através do seu sítio na *Internet*.
- Será incentivada uma abordagem de parceria pais/encarregados de educação e Colégio em relação à segurança digital em casa e no Colégio. Para esse efeito, poderão ser organizadas sessões para os pais/encarregados de educação com demonstrações e sugestões para uma utilização segura da *Internet* em casa ou serem aproveitados outros eventos em que os pais/encarregados de educação participam (como eventos desportivos) para abordar a segurança digital.
- Será solicitado aos pais/encarregados de educação que leiam e debatam a Política de Utilização Aceitável do Colégio, e respetivas implicações, com os seus filhos.
- Será disponibilizada informação e orientações aos pais/encarregados de educação sobre segurança digital em diferentes formatos.
- Serão disponibilizadas informações aos pais/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*.

7. PRESENÇA DO COLÉGIO NA *INTERNET*

Discussão:

Visto que a *Internet* é um meio vasto e de fácil transmissão de informação, cabe ao Colégio ter controlo sobre tudo o que é publicado acerca deste. A presença do próprio Colégio nas redes sociais poderá também ser importante, visto que é um meio de aproximação entre o Colégio e os pais/encarregados de educação.

Declarações:

- Cabe ao Gabinete de Comunicação e Imagem a responsabilidade de verificar periodicamente os conteúdos publicados nas redes sociais

- Cabe também ao Gabinete de Comunicação e Imagem a responsabilidade de monitorizar a reputação do Colégio na *Internet*.

8. POLÍTICAS DE UTILIZAÇÃO ACEITÁVEL

- Compreendo que a utilização de nomes de utilizador e palavras-passe para aceder à rede do Colégio deverá ser obrigatória.
- Comprometo-me a não revelar a minha *password* a ninguém e a alterá-la quando solicitado.
- Os sistemas de informação do Colégio devem ser utilizados de forma adequada. Tenho conhecimento de que, ao abrigo da lei portuguesa e das diretivas europeias, obter acesso não autorizado a material informático constitui uma infração punível por lei.
- Aceito que todos os equipamentos e programas informáticos disponibilizados pelo Colégio, só podem ser utilizados para fins relacionados com este.
- A fim de evitar o acesso não autorizado a sistemas ou a dados pessoais, não deixarei qualquer sistema informático ligado sem que seja necessário iniciar sessão com palavra-passe ou sem encerrar a minha sessão, consoante o caso.
- Comprometo-me a utilizar o *e-mail* institucional apenas para fins relacionados com o Colégio.
- Comprometo-me a informar imediatamente o professor designado para o efeito caso receba mensagens ofensivas.
- Comprometo-me a não tentar instalar qualquer equipamento nem qualquer programa adquirido ou descarregado, nomeadamente barras de ferramentas de *browsers*, sem permissão do responsável pelo sistema.
- Comprometo-me a respeitar os direitos de propriedade intelectual e de proteção de dados pessoais.
- Comprometo-me a ter responsabilidade ao usar dispositivos móveis que possam conter dados confidenciais (ex. *Pen's*) e a ter cópias de segurança noutro local.
- Comprometo-me a armazenar documentos oficiais (ex. atas de reuniões) na *cloud* do Colégio, garantindo a confidencialidade destes dados.
- Compreendo que o uso da *Internet* e de outras tecnologias relacionadas possam ser monitorizadas e gravadas.
- Compreendo que o acesso à *Internet* é um direito para quem demonstre responsabilidade e maturidade na sua utilização e que o seu acesso poderá ser recusado se tal não se verificar.
- Compreendo que sou responsável pelo meu comportamento quando uso a *Internet*.

Isto inclui os recursos e a linguagem que uso. Tenho, portanto, que assumir responsabilidade pela minha utilização da *Internet*, não a usando para fins incorretos ou ilícitos.

- Compreendo que a partilha de fotografias e filmes feitos no recinto Colégio, nas redes sociais, poderá trazer implicações graves no que toca à privacidade de todos os que nestes aparecerem.
- Compreendo que os ficheiros guardados na rede do Colégio poderão ser verificados com regularidade, de forma a identificar a existência que algum tipo de *Malware* (Vírus, *Trojans*, etc.).
- Compreendo que o acesso à *Internet* fornecido pelo Colégio incluirá sistemas de filtragem.
- Compreendo que estas regras foram feitas para me manter em segurança e que, não sendo seguidas, estarei a infringir o Regulamento Interno.