Cyber Sécurité à Highgate School

Les mesures pour assurer la cyber sécurité à Highgate School sont basées sur les valeurs essentielles de notre école. Pour nous aider à améliorer l'apprentissage de l'utilisation en toute sécurité des technologies de l'informatique et de communication (TICs), nous fournissons ce qui suit pour votre information.

Des pratiques rigoureuses de cyber sécurité sont en place, ce qui inclut les accords de cyber sécurité pour le personnel et les élèves. L'éducation de la protection de l'enfant, tel que le cursus the 'Keeping Safe Child Protection', inclut des informations concernant comment rester en sécurité quand on utilise des nouvelles technologies. Ces informations sont à la disposition de tous les élèves.

Le réseau informatique, les installations d'accès à l'internet, les ordinateurs et tous autres équipements/appareil TIC apportent des avantages immenses a l'enseignement et l'apprentissage a Highgate School, et pour le fonctionnement efficace de l'école. L'équipement TIC a un but éducatif approprié à cet environnement, que ce soit possédé ou loué partiellement ou complètement par l'école, et utilise soit sur ou hors du site.

Le but global de Highgate School est de créer et maintenir une culture de cyber sécurité qui reflète nos valeurs et qui soit en accord avec les obligations législatives et professionnelles.

Le matériel envoyé et reçu en utilisant le réseau peut être surveillé et filtré et / ou un logiciel de surveillance peut être utilisé pour restreindre l'accès à certains sites et données, ceci inclut les courriers électroniques. Dans les cas où un élève est soupçonné d'un crime, ceci sera signalé à la Police de l'Australie Méridionale. Dans les cas où un appareil électronique personnel tel qu'un portable est utilisé pour prendre des photo d'un crime, comme une agression, l'appareil sera confisqué et remis à la police.

Bien que tous les efforts raisonnables soient faits par les écoles et les administrateurs du DfE (Department for Education) pour empêcher l'exposition a des contenus inappropriés pendant l'utilisation des services en ligne du département, il est impossible d'éliminer complètement tous les risques. En particulier, le DfE ne peut pas filtrer le contenu de l'Internet accéder à la maison par votre enfant, de toutes autres locations qui ne sont pas l'école ou sur tous autres appareils qui appartiennent à votre enfant. DfE vous recommande l'utilisation d'un logiciel de filtrage approprié.

Plus d'informations concernant le filtrage de l'internet peuvent être trouvées sur les sites suivants

Australian Communications and Media Authority	http://www.acma.gov.au
NetAlert	http://www.netalert.gov.au
The Kids Helpline	http://www.kidshelp.com.au
Bullying No Way	http://bullyingnoway.com.au

Merci de contacter le proviseur, si vous avez des préoccupations à propos de la sécurité de votre enfant en ce qui concerne l'utilisation de l'internet et des appareils / équipements TIC.

Terminologies importantes

'Cyber sécurité' l'utilisation en toute sécurité de l'internet ainsi que des appareils / équipements. Ceci inclut les portables.

'Harcèlement sur internet' harcèlement avec l'utilisation de e-technologie pour la victimisation des autres. C'est l'utilisation d'un service internet ou de technologies portables – tels que les méls, les groupes de discussion tchat, messageries instantanées, pages Web ou textos – avec l'intention de nuire à autrui.

'TIC appareils / équipements' inclut les ordinateurs (tels que ordinateurs de bureau, ordinateurs portables, agenda électronique personnel), les périphériques de stockage (tels que clé USB et appareil de mémoire flash), cameras (tels que cameras vidéos et digitales et webcams), tous types de jeux sur portable, consoles de jeux vidéo, lecteurs/récepteurs vidéo/audio et tous autres technologies similaires.

'Matériel inapproprié' matériel qui traite de sujets tels que le sexe, la cruauté ou violence qui est probablement préjudiciable envers les enfants ou incompatible avec l'environnement scolaire.

'E-crime' se produit quand un ordinateur ou tous autres équipements / appareils de communication électroniques (i.e. internet, portables) sont utilisés pour commettre une offense, sont ciblés dans une offense, ou sont utilisés pour le stockage d'une offense.

Stratégies pour aider à garder les élèves de Highgate School cyber-sécure

Les parents et les gardiens jouent un rôle critique pour développer le savoir, la compréhension et l'éthique en ce qui concerne la sécurité et les pratiques sécurisées à toutes heures de la journée. Être cyber-sécure n'est pas une exception et nous vous invitons à parler à votre enfant des stratégies ci-dessous pour nous aider à rester sécurité avec l'utilisation de TIC à l'école et hors des heures d'école.

1. Je n'utiliserai pas l'équipement TIC de l'école jusqu'à ce que mes parents / gardiens et moi-même ayons signé et rendu le Cyber-Safety Use Agreement qui est sur le formulaire de consentement général.

2. Je n'utiliserai les ordinateurs et tous autres équipements TIC que pour mon apprentissage.

3. Je n'utiliserai l'internet à l'école que quand un/e enseignant/e me donnera la permission et qu'un adulte sera présent.

4. En cas d'incertitude à savoir si j'ai le droit de faire quelque chose qui implique TIC, je demanderai à un/e enseignant/e d'abord.

5. Si j'ai mon propre nom d'utilisateur, je m'identifierai en utilisant seulement ce nom. Je ne permettrai à personne d'utiliser mes identifiants.

6. Je garderai mes identifiants secret.

7. J'utiliserai l'internet, les méls, les portables ou tous autres équipements TIC seulement dans un but positif et non pas pour être méchant, grossier ou offensif, ou pour harceler, ou pour nuire à qui que ce soit, ou l'école même, et ce même si l'intention est de faire une blague.

8. Quand je suis à l'école :

   - Je tenterai de faire des recherches en ligne qui sont acceptables au sein de notre école. Ceci exclurait tout ce qui est grossier ou violent ou qui utilise un langage inapproprié tel que les jurons.
   - Je rapporterai toutes tentatives de contourner la sécurité, la surveillance et le filtrage qui sont mis en place à notre école.

9. Si je trouve quoique ce soit qui me contrarie, qui est grossier ou méchant, ou que je sais n'est pas acceptable à notre école :

   - Je ne le montrerai pas à d'autres.
   - J'éteindrai mon écran.
   - Je demanderai le soutien d'un/e enseignant/e immédiatement.

10. Je n'apporterai aucun équipement/appareil TIC que ce soit à l'école sans une permission écrite de la maison et de l'école. Ceci inclut les portables, les iPods, les jeux, les caméras, et les clés USB / lecteurs portables.

11. Je ne connecterai aucun appareil TIC que ce soit au TIC de l'école sans la permission écrite de l'enseignant/e, ou n'exécuterai un logiciel (i.e. clé USB / lecteur portable, camera ou portable). Ceci inclut toutes technologies sans fil / Bluetooth.

12. Les stratégies de cyber sécurité de l'école sont applicables à tous TICs apporté à l'école.

13. Afin de pouvoir assurer ma conformité avec les lois de droits d'auteur, je ne téléchargerai ou copierai aucun fichier que ce soit tels que la musique, les vidéos, les jeux ou programmes sans la permission d'un/e enseignant/e ou l'auteur du matériel originel.

14. Je demanderai la permission de mon enseignant/e avant d'ajouter toutes informations personnelles en ligne. Ceci inclut :

   - Mon prénom et mon nom de famille
   - Mon adresse
   - Mon adresse électronique
   - Mes numéros de téléphone
   - Des photos de moi-même et/ou de gens dans mon entourage immédiat

15. Je respecterai tous TICs appartenant à l'école et je les traiterai avec soin. Ceci inclut :
    - Ne pas interrompre de manière intentionnelle le bon fonctionnement des systèmes TICs de l'école.
    - Ne pas essayer de pirater ou d'obtenir un accès non-autorisé à tous les systèmes.
    - Suivre toutes les stratégies de cyber sécurité de l'école, et ne pas participer si d'autres élèves choisissent d'être irresponsable avec TIC.
    - Rapporter tous bris / dommages à un membre du personnel.

16. Si je ne suis pas les pratiques de cyber sécurité l'école peut en informer mes parents / gardiens. Dans les cas sérieux, l'école peut prendre des actions disciplinaires envers moi. Ma famille peut être tenue responsable des coûts de réparation. Si du matériel ou des activités illégaux sont impliqués ou un e-crime est soupçonné, il peut être nécessaire d'en informer la police et de garder de manière sécurisée les articles personnels pour qu'ils soient potentiellement inspecter par la police. Ceci peut être le cas même si l'incident se produit hors site et/ou en dehors des heures de classe.