香港自閉症聯盟 - 有關 Zoom 網上課程資訊安全注意事項

1/ 前言：

本文乃「香港自閉症聯盟」下簡稱「聯盟」就選取 Zoom App 雲端視像會議軟件 (下簡稱 Zoom) 提供網上課程，予學員作在職/持續培訓和普及教育的注意事項，有關內容乃參考自網絡及網上私隱安全專業團體及專家就 Zoom 網上教學意見而整理，本文僅供學員作一般性參考用途，讀者如有進一步需要，請自行諮詢相關專業團體/人士意見，本「聯盟」、課程合作伙伴及其供應商等並不會負責因本文內所涉及學員因參加聯盟課程可能直接及或間接引致學員在網絡安全及或私隱保障方面造成的損失及或法律糾紛及訴訟等事宜索償及或承擔賠償責任。

2/ 對象：

本文內容只適用於香港區已經繳費報讀「聯盟」以 Zoom 開辦網上課程的學員。其他香港以外地區的 Zoom 網上課程學員，請按居住地區的網絡及或個人網絡私隱安全狀況，自行考慮其他相關因素。

3/ 聯盟 Zoom 網上課程的網絡安全及個人私隱保障措施：

3.1 聯盟所有網上課程將按香港個人私隱法例要求處理及保存收集的個人資料；

3.2 聯盟保證不會出售課程學員的個人資料和數據予第三者；

3.3 聯盟不會在 Zoom 軟件供應商雲端儲存、出售及或分享課程學員的個人資料；

3.4 聯盟進行網上課程時，會設定不同的課室(會議室)代號(ID) 及登入課室密碼 (password)；

3.5 聯盟邀請網上課程學員時，課室的連結與登入課室密碼，將使用不同電郵寄出；

3.6 在網上課程舉行期間，只有課程主持人才可以分享螢幕畫面權限；

3.7 如果有需要我們會設立等候室，以加強審核課程學員進入課室的資格；

3.8 在網上課程舉行一段時間後(按不同的課堂性質而決定)，我們可能會關閉課室(會議室)，以防止惡意 Zoom Bombing 的干擾；

3.9 聯盟保證不會分享或發送 Zoom 網上課程學員專注監察功能紀錄(Attention Tracking) 予第三者；

3.10 聯盟在宣傳相關 Zoom 網上課程時，已清楚註明部份課程將會被錄影以供學員課後網上重温，並會在每堂錄影 Zoom 網上課程前，通知所有學員及取得其同意，進行錄影

3.11 聯盟在 Zoom 網上課程舉行前，會通知學員可以關閉個人視頻或可識別個人身份頭像，以避免課堂錄影時存錄其面容或頭像。

4/ 建議參加聯盟 Zoom 網上課程學員注意事項：

4.1 學員必須從 Zoom 官方網頁 (www.zoom.us) 下載軟體，及定期更新最新版本程式。

4.2 使用 Zoom 上課時， 請勿關閉點對點加密預設功能。

4.3 在登入 Zoom 個人帳户，不宜使用原有 Facebook 或 Google 帳號及使用相同密碼登入其 Zoom 帳户。

4.4 請勿把網上課堂的會議室鏈接及密碼，向非相關人士或在公開的社交媒體發佈。

4.5 如果你本身工作已擁有一個 Zoom 個人免費或商業帳户，並需要在該原有帳户，進行高保密性及或敏感性工作；建議你在參加聯盟 Zoom 網上課程時，在自己電腦/手機的作業系統中，另外開設一個 Zoom

個人免費使用者帳户，及設置不同的帳户登入密碼，並使用這專述者帳户去參加聯盟 Zoom 網上課程，在網上課程結束後，再切換為原本的使用者帳户執行本身高保密性及或敏感性工作。

4.6 你在參加聯盟 Zoom 網上課程時，可以選擇把個人端視頻及可識別個人身份頭像關閉，同時亦可以另行設置參加者代號，以保障你的網絡個人私隱。

4.7 根據 2019 年某資安刊物報導， Mac 電腦用戶在應用 Zoom 曾經出現資安漏洞， Zoom 在未經過使用者同意下，可以自動開啟其 Mac 電腦鏡頭（註 1）。據悉該 Zoom 功能已經在程式更新後解決該資安漏洞。

4.8 根據資安人士報導，在安卓系統 (Android) 運行的智能手機或平板電腦等設備上使用 Zoom，比較在 Mac 或 Windows 桌上或手提電腦上使用 Zoom 較安全 (註 2 及註 3)。

4.9 根據網络保安專家意見，使用者必需要為所有聯接外界裝置安裝防毒軟件及定期更新。瀏覽互聯網時不應下載來歷不明的軟件/附件，使用電郵應小心垃圾及釣魚式病毒郵件 (phishing scams email)。

5/ **聯盟對目前(2020 年 4 至 5 月)使用 Zoom 進行網上課程的意見及決定**

5.1 聯盟在 2020 年 1 月初選擇 Zoom 作網上課程載具，乃經過諮詢專業人士意見、及進行多次課堂實測，最後建基於下列理據：(a) 軟體用家友善、(b)操作界面簡易、(c) 教學功能完備、(d) 市面普及性高、(e) 個人版免費可減輕學員學習支出、(f) 安裝簡便、(g) 方便性和資訊安全及保障私隱平衡、(h) 支援多介面和操作系統裝置、及 (i) 市場用户意見和認受性。而由 2020 年 3 月初至 4 月初，聯盟合共舉行了四次課堂和二次試課，約近 600 人參加上述課堂，均順利完成。

5.2 在實務上，聯盟 2020 年 4 至 5 月份，已經編排、宣傳及招募但尚未舉行，尚餘下二項主題課程(合共 6 堂 18 小時) ，及壹個單項講座(1 堂共 2 小時)，各項網課亦已經有超過 120 人報名及繳費，如果要在短短開課前四至九天內 (AVT-4A 課程在 4 月 18 日及 WAAD-1B 講座在 4 月 23 日開課) ，和開課前二星期(ABA-4A 課程在 5 月 2 日開)，重新更換其他雲端會議軟件，去進行該批網上課程及講座，無論在聯盟主辦方的技術支援，或是對已繳費報名學員亦需要重新安裝相關網課操作軟件、試用及課堂操練等方面，均可能面對不少技術和運作困難。此舉既違反聯盟對已報名及繳費學員的承諾，更可能引致大量學員退出網課和要求退款申訴。

5.2 故此，聯盟決定 2020 年 4 至 5 月份，餘下已經編排的二項主題課程，及壹個單項講座，均會按原訂計劃，採用 Zoom 軟件授課。但聯盟會加強本文上述第 3.4 至 3.11 項等網絡安全措施，並希望各學員體諒因此等新增措施帶來的不便，先致歉意。

5.3 對於社會人士及業界團體熱切關注網上教學資安，建議聯盟考慮改用市場上其他現存的通訊或雲端會議軟件，例如：Adobe Connect, Cisco WebEx, CybertLink U Meeting, Global Meet, Google Hangouts Meet, Jitsi Meet, Microsoft Teams, Rocket Chat, & Sandstrom 等軟件，聯盟現已成立「網絡安全工作小組」，並與合作伙伴研究相關議題，儘可能在 5 月中或以前作出決定及公佈，2020 年 6 至 12 月份策劃中的網上課程運作軟件考慮。

5.3 聯盟和各位同樣重視及致力維護網上課程安全安及保障個人私隱，據專家審視現存網絡安全的領域中，似乎並不存在具有 100%保證網絡及私隱安全的軟體，還需有賴網上課程提供者和使用者保持高度敏銳性和安全意識。讓我們攜手在網上課程的方便性及網絡安全兩端，取得最大的平衡和得益。如果你對本文有任何意見，歡迎你電郵聯絡我們 info@autism.hk ，或瀏覽「香港自閉症聯盟」右列網址 www.autism.hk 。

香港自閉症聯盟

2020 年 4 月 13 日

參考資料來源：

註 1 ：鄧天心 (2019). 驚爆資安漏洞！視訊會議軟體 Zoom 能偷偷開啟 Mac. 新頭殼 newtalk (July, 2019)

註 2 ：李建興(2019). Zoom 緊急修正 Mac 客戶端漏洞，拿掉本地主機網頁伺服器， iThome (July 10, 2019)：

註 3 ：Chen, Brian X., (2020). 使用 Zoom，風險自負，紐約時報中文網 2020 年 4 月 9 日 https://cn.nytimes.com/technology/20200409/zoom-privacy-lessons/zh-hant/

Hautala, Laura. (2020). Working from home makes you vulnerable to hackers. Here's how to stay safe. In CNET, 25 March 2020. Accessed at 10 April 2020. https://www.cnet.com/news/working-from-home-makes-you-vulnerable-to-hackers-heres-how-to-stay-safe/

Hodge, Rae. (2020a). Using Zoom while working from home? Here are the privacy risks to watch out for. In CNET, 2, April 2020. Accessed at 10 April 2020 https://www.cnet.com/news/using-zoom-while-working-from-home-here-are-the-privacy-risks-to-watch-out-for/

Hodge, Rae. (2020b) Zoom: Every security issue uncovered in the video chat app. In CNET, 9 April 2020. Accessed at 10 April 2020. https://www.cnet.com/news/zoom-every-security-issue-uncovered-in-the-video-chat-app/

Priscilla Barolo, Zoom Inc. (May 7, 2019): Zoom Achieves FedRAMP Moderate Authorization

XY Wang, PANDA!YOO (March 10, 2020): Zoom! You are using the video conference application (mostly) developed by Chinese.

Zak Doffman, Forbes (Jan 28, 2020): New Zoom Security Warning: Your Video Calls At Risk From Hackers — Here’ s What You Do.

Zoom or Government, https://zoomgov.com