

科技教育學習領域 – 資訊及通訊科技科

國家安全教育課程框架（2025）

引言

此課程框架¹以表列形式展示資訊及通訊科技科的學習如何聯繫國家安全教育的相關學習元素，方便學校規劃國家安全教育的學習內容。學校須以「有機結合」、「自然連繫」、「多元策略」、「互相配合」、「課堂內外」及「全校參與」的方式，把國家安全教育融入本科的課程規劃和學與教中。除本課程框架外，學校亦應參考《香港國家安全教育課程框架》（2025）和其他相關課程文件，以更好地落實國家安全教育。

1. 整體教學重點

- 1.1 資訊及通訊科技是處理資訊所需的科技，包括資訊的創造、處理、儲存、獲取及溝通。在知識日新月異、趨向跨學科，以及資訊爆炸的現代社會，資訊及通訊科技實在是不可或缺的一環。
- 1.2 高中資訊及通訊科技課程的必修部分包含「資訊及通訊科技對社會的影響」和「互聯網及其應用」。「資訊及通訊科技對社會的影響」部分幫助學生理解及以道德角度分析使用資訊及通訊科技所帶來的各種問題，包括其在經濟、法律、社會、道德及保安等方面所構成的影響。「互聯網及其應用」部分包括上網的概念、互聯網服務及應用。學生亦要慎思明辨地分析網上取得資料的可靠性，並明白互聯網對社會上各種活動的影響，以及讓他們能夠有效及合乎道德地使用資訊及通訊科技，讓學生從負責任的網絡使用者角度了解數據安全、網絡安全、人工智能安全和科技安全的重要性。

¹ 本框架的內容以舉隅形式列出，學校應根據學生的學習需要和能力採用或調適相關建議。

1.3 學生透過本科的學習活動可更全面地明白數據安全和網絡安全的重要性，包括通過判斷資訊的真偽的學習經歷和認識傳播假資訊的後果，培養他們資訊素養能力，成為守法和負責任的公民。此外，教師通過與學生討論有關網上交易議題，讓他們關注數據安全和網絡安全。

2. 學習重點

科技教育學習領域－資訊及通訊科技科 〔第四學習階段（高中）〕		《香港國家安全教育課程框架》 (2025)
學習範疇（舉隅）	學習元素（舉隅）	相關學習元素／國家安全重點領域 （舉隅）
單元 C 互聯網及其應用 網上威脅及保安	- 描述常見網絡保安威脅所造成的潛在風險 - 學生應提議改善網絡保安的有效措施、討論網上潛在的私隱威脅，並建議保護私隱的方法 - 意識防止竊聽及資訊阻截的資訊加密技術 - 學生應懂得如何利用身份鑑定及授權程序來控制網上資料的存取、了解電子交易所採用的保安措施及認識保安措施的最新發展	4.9 加深認識國家和香港的科學和創新科技事業對維護國家安全和可持續發展的重要性 - 相關的國家安全重點領域：數據安全、網絡安全
單元 E 資訊及通訊科技對社會的影響 科技創新	- 了解科技創新的基本概念及其應用 - 學習人工智能 AI 和數據科學的圖形識別、三維打印技術、擴增實境 AR 和虛擬實境 VR，並認識國家在人工智能（包括生成式人工智能）方面的發展和成就	4.5 進一步認識和關心國家在各方面（例如：社會、經濟、國防、環境、外交、科技、醫療衛生、交通基建）的成就，並以國家的成就為榮 - 相關的國家安全重點領域：人工智能安全

科技教育學習領域 – 資訊及通訊科技科 〔第四學習階段（高中）〕		《香港國家安全教育課程框架》 (2025)
學習範疇（舉隅）	學習元素（舉隅）	相關學習元素／國家安全重點領域 (舉隅)
單元 E 資訊及通訊科技對社會的影響 健康及道德議題	- 認識公平存取的重要性 - 討論使用資訊及通訊科技時的道德考慮因素 - 學生應陳述互聯網上資訊自由的好處和壞處，他們還應從數碼隔閡、性別平等和殘障人士獲得機會等方面，以及從地區和全球角度，了解相關公平問題	4.8 進一步認識國家在發展過程中面對的挑戰和機遇，從而增強憂患意識，做到居安思危 - 相關的國家安全重點領域：數據安全、網絡安全
單元 E 資訊及通訊科技對社會的影響 知識產權	- 了解知識產權及版權的基本概念 - 從用戶和軟件開發商的角度出發，了解不同的軟件許可方式的好處及風險，例如免費軟件、共享軟件、開放源碼軟件及版權軟件 - 敘述侵犯軟件版權及互聯網上盜版的行為 - 學生認識能減少具知識產權的數碼財產被盜竊的方法及了解在香港侵犯版權（尤其是與教育有關的侵權行為）可引致的法律後果 - 學生應重視資訊素養和善用資訊及通訊科技，並	4.8 進一步認識國家在發展過程中面對的挑戰和機遇，從而增強憂患意識，做到居安思危 4.19 認識我國乃至世界各國人民在社會、道德、經濟、環境、科技等領域可能面臨的安全風險，並在相關議題上能夠作出明智的、合乎國家利益的決定及判斷

科技教育學習領域 – 資訊及通訊科技科 〔第四學習階段（高中）〕		《香港國家安全教育課程框架》 (2025)
學習範疇（舉隅）	學習元素（舉隅）	相關學習元素／國家安全重點領域 (舉隅)
	能分享知識，以及了解如何影響人們的決定，以至改變整個社會，培養他們使用資訊及通訊科技的責任感，並藉此建立正確的價值觀和態度 近年人工智能發展迅速，競爭激烈，學生可了解國家發展人工智能工具的情況，並了解維護國家的科技發展成果的重要性，除了保障國家發展利益外，亦可避免國家的科技發展受制於人	相關的國家安全重點領域：科技安全、網絡安全

3. 建議的學與教活動（舉隅）（高中）

以下僅屬舉隅，教師可因應校情及科本特色設計適合的活動，以推展國家安全教育。

✧ 課堂學習

- **【資訊的真偽課題】**分組研究教師指定的網上資訊，討論以不同的方法查證及指出該資訊的真偽，並評估錯誤傳播該資訊對社會的影響
- **【網上交易的安全】**分組研究用戶利用網上銀行戶口進行交易時，如何保障其安全性、身份認證，以及各持份者（例如用戶、政府、銀行、互聯網服務供應商）在保障網絡安全時的角色
 - 配合課程宗旨和目標，設計適切的自學活動，讓學生了解國家對科學與科技的安全議題的關注和重視
 - 可觀察瀏覽器顯示的資料，以確定網頁及其資料的安全性
 - 例如：我們在瀏覽器輸入網址 **www.aaa.bbb.ccc** 後，我們可觀察瀏覽器：
 1. 顯示的網址以 **https** 開始，即 **https://www.aaa.bbb.ccc...**，表示該網頁安全(Secure)
 2. 檢視網址左邊或右邊附帶的符號，網站安全狀態：
 - 安全
 - 資訊或不安全
 - 不安全或危險
 - 如果網址的 **bbb** 部份為 **gov**，表示該網站為政府網站，網頁中的資料可信。
- **【知識產權課題】**讓學生從用戶和軟件開發商的角度，分組辯論不同的軟件許可方式的好處及風險，例如免費軟件、共享軟件、開放源碼軟件及版權軟件，以加深對此課題的認識，並培養其對知識產權及版權概念的正確價值觀及積極態度，從而避免觸犯涉及數碼財產的知識產權的盜竊和侵權行為

✧ 延伸學習活動

- **【傳播假資訊的後果】**教師與同學一起閱讀、分析報章上傳播假資訊的真實個案，讓學生明白網上傳播假資訊者會因而負上刑責；我們要在網上謹言慎行，做個負責任的網民
- **【認識創科企業】**安排學生參觀香港和內地的科技園區／企業，認識不同創新科技事業和國家在科技發展的成就