

資訊素養與倫理 國中 5 版

編撰：臺北市立明德國民中學 葛允文組長 / 陳俊宏教師

虛擬世界任遨遊

數位安全零信任，科技生活不設限（上）



1-1 學習目標

- 認識「數位身分」、「數位分身」、「網路零信任」的技術原理與重要性。
- 探討「數位身分」、「數位分身」、「網路零信任」在各領域的應用及影響。
- 深入探討虛擬世界對生活與教育的影響與自我保護的方法。
- 學習如何平衡虛擬與現實生活，保持健康的心態與習慣。
- 培養對數位世界的批判思考能力與資訊倫理觀念。

► 核心素養

- 科-J-A1 具備良好的科技態度，並能應用科技知能，以啟發自我潛能。
- 科-J-B1 具備運用科技符號與運算思維進行日常生活的表達與溝通。
- 科-J-B2 理解資訊與科技的基本原理，具備媒體識讀的能力，並能了解人與科技、資訊、媒體的互動關係。
- 科-J-C1 理解科技與人文議題，培養科技發展衍生之守法觀念與公民意識。
- 科-J-C3 利用科技工具理解國內及全球科技發展現況或其他本土與國際事務。
- 社-J-A2 覺察人類生活相關議題，進而分析判斷及反思，並嘗試改善或解決問題。
- 社-J-B2 理解不同時空的科技與媒體發展和應用，增進媒體識讀能力，並思辨其在生活中可能帶來的衝突與影響。

► 學習表現

- 運t-IV-4能應用運算思維解析問題。
- 運p-IV-1 能選用適當的資訊科技組織思維，並進行有效的表達。
- 運a-IV-1能落實健康的數位使用習慣與態度。
- 設k-IV-2能了解科技產品的基本原理、發展歷程、與創新關鍵。
- 設k-IV-3能了解選用適當材料及正確工具的基本知識。
- 設a-IV-2能具有正確的科技價值觀，並適當的選用科技產品。
- 設c-IV-1能運用設計流程，實際設計並製作科技產品以解決問題。
- 設c-IV-2能在實作活動中展現創新思考的能力。
- 社1b-IV-1應用社會領域內容知識解析生活經驗或社會現象。
- 社3a-IV-1發現不同時空脈絡中的人類生活問題，並進行探究。

► 學習內容

- 資A-IV-1 演算法基本概念。
- 資S-IV-3 網路技術的概念與介紹。
- 資H-IV-1 個人資料保護。
- 資H-IV-2 資訊科技合理使用原則。
- 資H-IV-3 資訊安全。
- 資H-IV-4 媒體與資訊科技相關社會議題。
- 資H-IV-5 資訊倫理與法律。
- 資H-IV-6 資訊科技對人類生活之影響。
- 公Bj-IV-3 侵權行為的概念與責任。
- 公Bj-IV-4 智慧財產權為什麼需要保障？日常生活中，如何合理使用他人的著作？侵害著作權須負的法律責任有哪些？
- 公De-IV-1 科技發展如何改變我們的日常生活？

► 學習重點

- 認知「數位身分」、「數位分身」、「網路零信任」的原理與重要性。
- 了解「數位身分」、「數位分身」、「網路零信任」在不同領域的應用，並分析其優勢與限制。
- 探討「數位身分」、「數位分身」、「網路零信任」在數位環境中相關法律與如何保護自身安全。
- 深入探討虛擬世界對生活及教育的影響，並學習如何平衡虛擬與現實生活，保持健康的心態與習慣。



1-2 引起動機

01



這個角色太帥了！
比現實中的我還厲害！



02

你知道嗎？這個遊戲角色可以
說是你的「數位分身」，它代表
著虛擬世界中的你。



03



等等...我的社群平台頭像、聊天貼圖、遊戲角色...這些都是我的數位分身嗎？那真正的我是哪一個？

04

數位分身就像鏡子的反射，可以展現不同面向的你，但真實的你永遠是這些分身背後的創造者和控制者！



＊數位分身可以展現理想中的自己，但別忘了與真實世界保持連結！

動動腦，想一想

1. 你的數位分身（遊戲角色、社群頭像等）與真實的你有何相似或不同？為什麼？
2. 未來科技發展下，你認為數位分身可能會如何演變？這會帶來哪些機會和挑戰？

我們每天都在虛擬與實體世界之間穿梭，當你在手機上玩遊戲、使用社群軟體或是線上購物時，你都在建立自己的「數位身分」和「數位分身」。

「數位身分」就像是你在網路世界的身份證，包含了你的帳號、密碼和個人資料；而「數位分身」則像是虛擬世界中的你，可能是遊戲角色、社群媒體上的形象，或是聊天機器人中模擬你說話方式的AI助手。

隨著技術的發展，保護這些「數位身分」變得格外重要。「網路零信任」是一種新的安全觀念，就像學校門口的警衛一樣，不管認不認識你，每次進入都需要出示證件，以確保安全。

【數位身分是什麼？】

數位身分就像你在網路世界的「身分證」，包括：

- 你的帳號名稱和密碼
- 電子郵件地址
- 個人資料（如生日、興趣）
- 在網路上的活動紀錄

「數位分身」就像你在網路世界裡的「虛擬雙胞胎」！想像一下，你有一個住在電腦或手機裡的「分身」，它會模仿你的行為、紀錄你的習慣，甚至能幫你做一些事情。

【數位分身是什麼？】

- 你在遊戲裡的角色（會跟著你跑跳、買裝備）
- 社群軟體上的帳號（貼文、按讚的紀錄）
- 手機裡的語音助理（回答問題的「聲音版」的你）
- AI生成的模擬形象

為什麼需要「數位分身」？

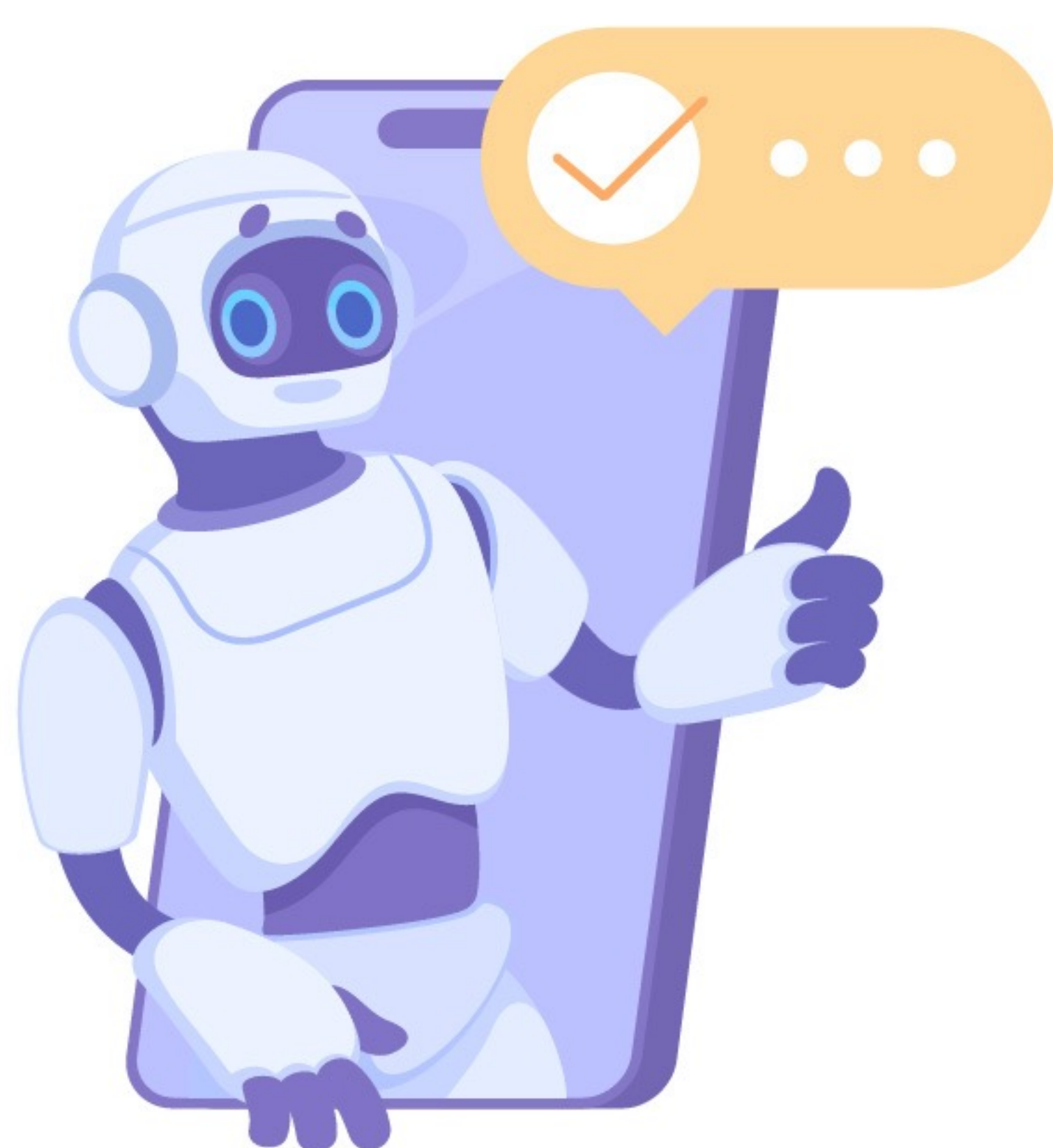
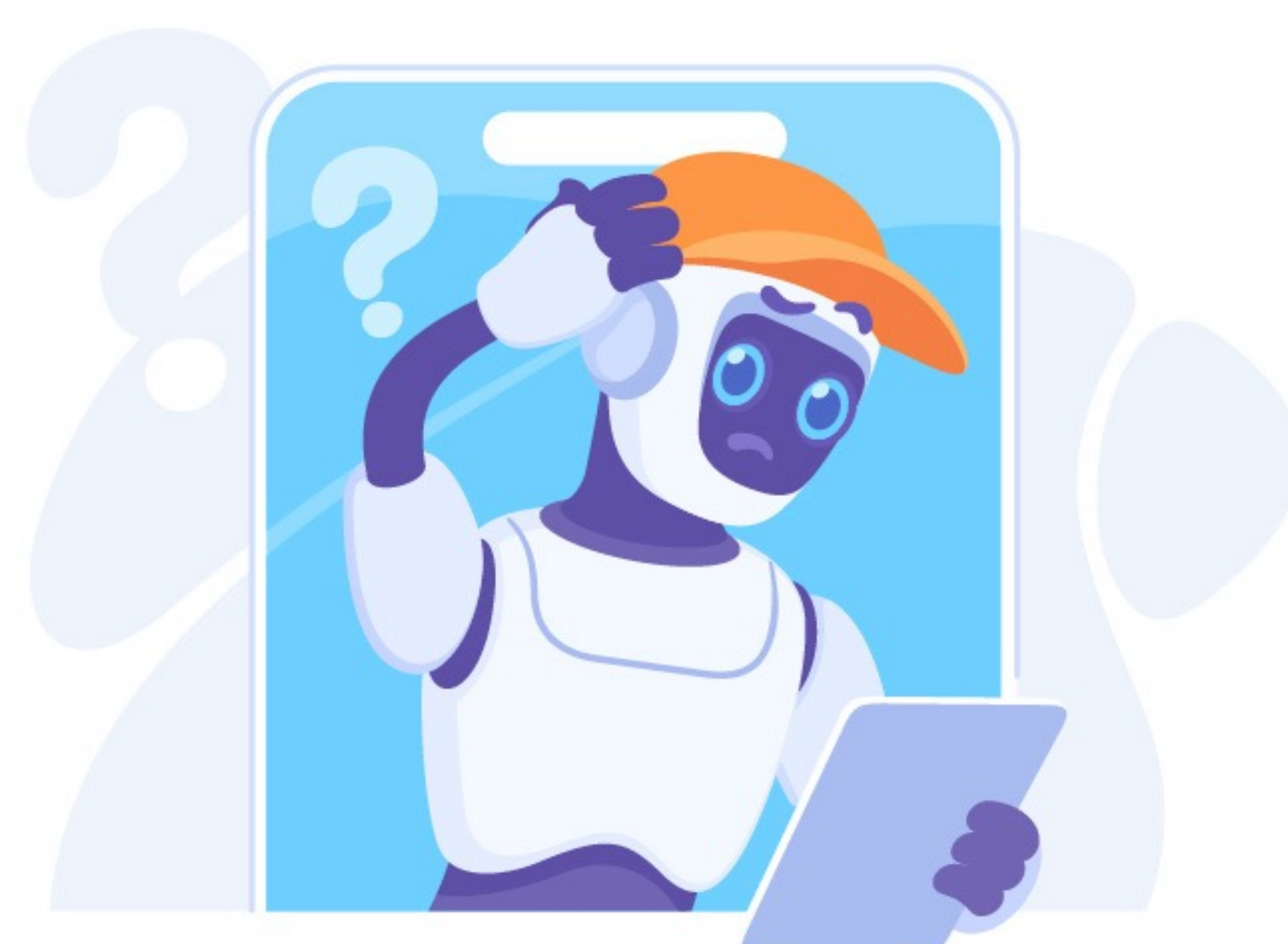
就像玩遊戲時，角色越強就能打敗更多怪物一樣，數位分身越了解你，就越能幫你節省時間、解決問題！例如：醫生用病人的數位分身模擬治療效果、工程師用數位分身測試機器會不會故障、如何改進、改良讓機器更耐用等。

數位分身是利用科技在虛擬世界中創造的擬真個體，可以有很多種類型，比如用數據分析來做精準行銷的分身、模擬醫療診斷的分身，以及線上遊戲裡的虛擬角色等；不同的分身可以用於學習、娛樂、商業和醫療等多個方面，雖然這樣的技術帶來了許多便利，但也帶來了新的安全隱患。

「零信任網路架構」(Zero Trust Network Architecture, ZTNA) 是一種解決方案，它假設任何網路或裝置都是不安全的，對每次的存取請求進行嚴格的檢查，這樣可以有效減少網路或裝置的威脅和資料外洩的風險。

另外，在虛擬世界任遨遊（下）的課程單元中，我們將更進一步探索「區塊鏈」(blockchain) 的技術，它提供了一種去中心化、透明且不可竄改特性，亦能提升數位身分安全。它能建立安全的數位身分管理系統，讓使用者更好地控制個人資料，防止身分盜用和資料偽造，實現另類的數位分身和網路零信任的概念。

本單元將帶領大家探索網路世界的奇妙，特別是數位身分、數位分身及網路零信任等相關概念的基礎知識及其應用方式。在這個過程中，我們將深入探討這些技術如何影響個人和組織在虛擬空間中的行為，以及如何確保這些數位資料安全無虞。



2-1 主題探索

A.1、數位身分的基本概念

數位身分指的是一個人在數位平台上所擁有的身分和存在，這包括了用戶在網路上所產生的資料和行為。數位身分通常由個人資訊（如姓名、電子郵件地址）、社交媒體帳戶、線上活動紀錄（如瀏覽歷史和購物習慣）等各種獨特的識別符號所組成。

隨著科技的發展，數位身分已經不再只是簡單的身分認證，而是個人在網路空間中建立和維護的多種虛擬形象。

A.2、數位身分的主要類型：

- 電子郵件地址：
作為數位身分的核心標誌之一，常見於企業和組織的官方網站以及個人社交媒體帳號。
- 帳戶名稱：
如社交媒體帳號（如Facebook、LINE等）或個人網路平台的帳號，用來區分不同用戶和內容。
- 身分識別符號：
例如銀行帳號、信用卡卡號、健保卡卡號等，這些在現實生活交易中常見的身分識別資料，在網路世界也扮演著重要角色。
- 網路服務使用者名稱：
如Google、Apple等公司提供的服務帳號，用戶透過這些帳戶進行日常操作和資訊管理。

A.3、數位身分的重要性和影響：

- 身分認證：
數位身分在網路交易和互動中有著關鍵作用，它確保了個體的身分真實性，從而保護隱私並防止欺詐行為。
- 信任建立：
特別是在網際網路環境下進行合作和交易時，更能彼此信任並確保安全。。
- 隱私保護：
對於個人而言，良好的數位身管理有助於保護隱私。例如，用戶可以控制哪些第三方能夠訪問其數位身分資料以及如何使用這些資料。
- 個性化體驗：
企業利用個體的身分來提供更加個人化（personalized）和相關（relevant）的服務和產品，促進更好的溝通和互動。



A.4、維護數位身分的重要性：

- 密碼管理：
持強健且獨特的密碼是保護數位身分的第一步，定期更改密碼並考慮使用複雜性的密碼或多重認證。
- 更新個人資料：
確保所有相關帳戶和服務的個人資訊都是最新和正確的，這樣可以防止身分盜用和欺詐行為。
- 監控異常活動：
密切關注自己數位身分下的帳號和伺服器登入等活動，如果發現任何不尋常的活動或可疑行為，應立即更改密碼，並向師長或相關單位回報。。

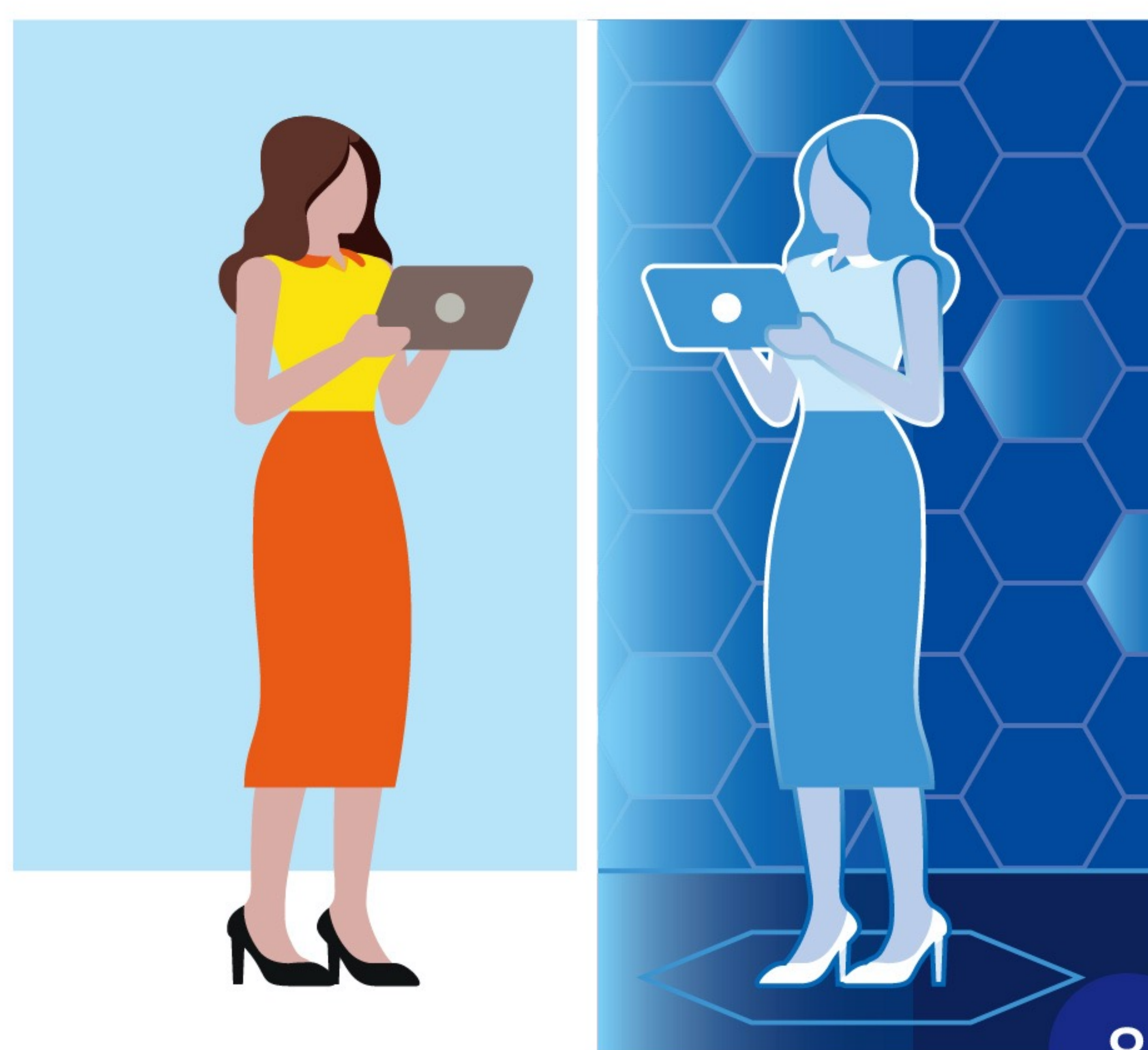
數位身分是個體在現代資訊社會中的重要組成部分，它們不僅為個人提供了便利的操作體驗，還確保了網路環境的安全性和可信度。透過有效地管理和維護自己的數位身分，可以最大限度地發揮這些技術的潛力，從而實現更安全、便捷和個性化的數位生活。



B.1、數位分身的基本概念

數位分身（Digital Twin）是指使用電腦技術在虛擬世界中創建的擬真個體，這些個體基於真實世界中的個人或物體的特徵、行為、數據和互動模式所生成，藉以模擬在現實世界中的個體、物體或系統。

數位分身可反映出個人的外貌、個性，以及網路上的活動與歷史，為使用者提供一種更加沉浸式的體驗，並在各種數位平台上進行互動和表達，這個虛擬的複製品也可以設定成具有自己的特性、行為和反應，讓使用者可以在虛擬環境中進行互動和模擬行為。



B.2、數位分身可以做什麼？

- 學習你的習慣：例如智慧手錶記錄你每天走了幾步、幾點睡覺。
- 代替你處理事情：例如聊天機器人幫你回答常見問題。
- 預測你的需求：例如線上課程推薦「你可能會喜歡的影片」。

B.3、數位分身的主要類型：

- 社交媒體分身：
在社交網站上展示個人形象及風格的虛擬角色。
- 遊戲虛擬角色：
在線上遊戲中的角色，玩家可根據個人喜好自訂外觀及技能。
- 虛擬物體：
虛擬物體是指使用電腦技術創造一個虛擬的物體，具有自己的形狀、大小和材質。
- 虛擬系統應用於工、商業等分身：
虛擬系統是指使用電腦技術創造一個虛擬的系統，具有自己的結構、功能和行為，例如：利用數據分析生成的虛擬顧客，以提升行銷策略的有效性。
- 虛擬助手或聊天機器人：
能模擬人類對話和行為的數位助理，幫助用戶解決問題。

B.4、數位分身的重要性和影響：

- 個人化體驗：增強線上互動的個性化與趣味性，吸引更多使用者參與。
- 數據收集與分析：幫助企業了解消費者行為，提升產品和服務的品質。
- 網路安全：正確管理數位身分能防止身分盜用和網路詐騙。
- 教育與培訓：透過模擬學習，提升學習效果，讓學生在虛擬環境中進行實作。
- 隱私保護：使用者可以透過設定強密碼、啟用雙重驗證或定期檢查帳號登入紀錄等方式，管理自己的數位分身，確保個人資料安全。

B.5、維護數位分身的重要性：

- 定期更新形象和內容：
保持數位分身的形象和內容與用戶的實際外貌一致，並根據需要進行更新。
- 控制訪問權限：
確保只有授權的用戶可以查看或修改數位分身的內容，以保護隱私。
- 管理互動行為：
引導或監督數位分身的網路上互動行為，以維護品牌形象和用戶體驗。

數位分身是現代資訊社會中的新興技術，它們為個體提供了在虛擬世界中展示自己形象的新方式，透過有效地管理和利用數位分身，個人和企業可以提升品牌價值、增強互動性和個性化行銷效果。然而，在享受數位分身帶來的便利時，也需要注意保護個人隱私和品牌形象，了解這些基本概念及其應用將有助於我們更好地利用數位科技。

C.1、數位分身的應用

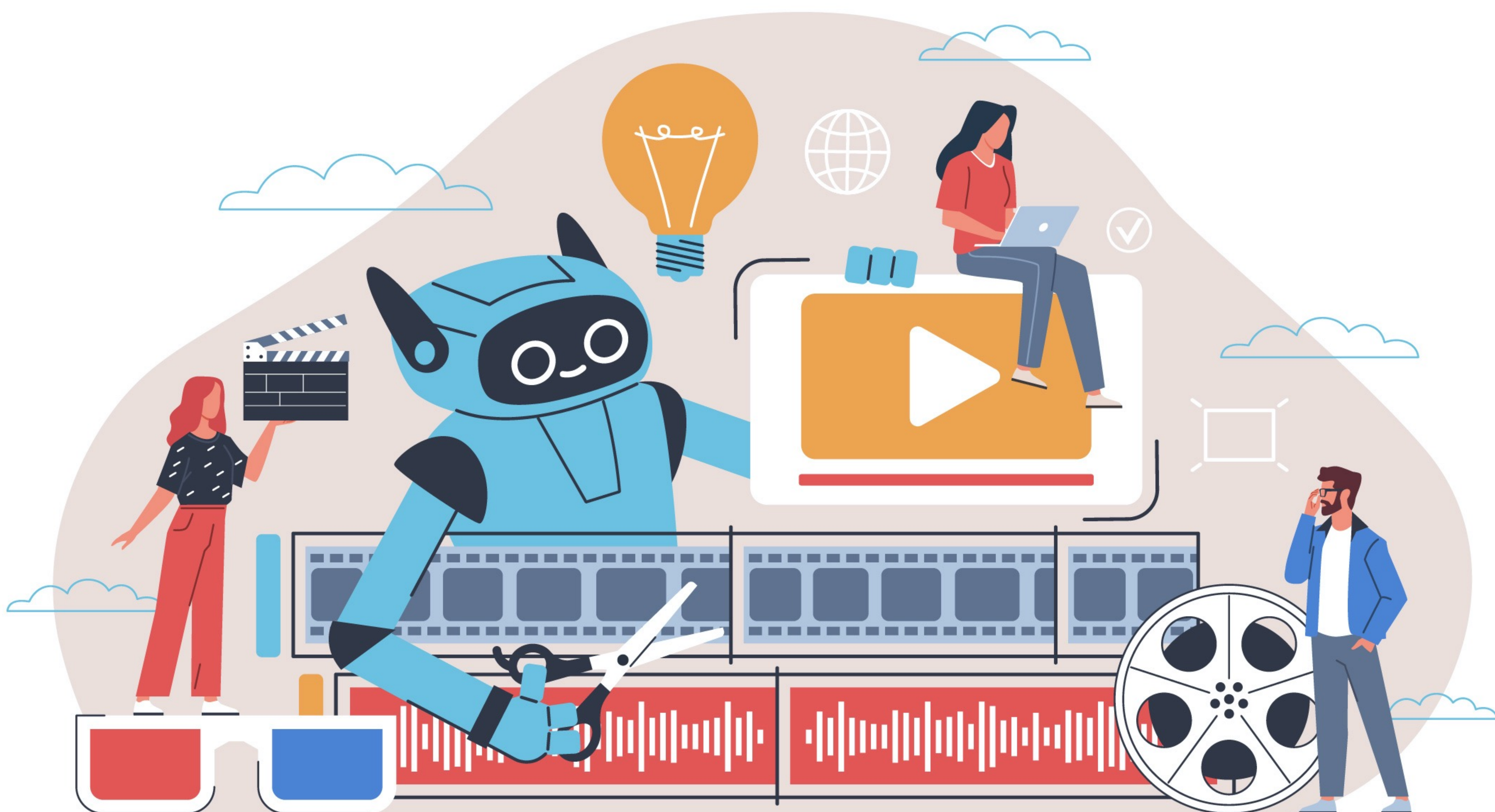
ChatGPT於2022年12月推出至今，已被廣泛的運用於各領域，各種軟體系統，如影音串流網站、電商，或你每天用的文書軟體，都會有擬人化的AI代理人（AI Agent），你只要開口，它就幫你解決所有問題。

舉例來說，以前歌手、明星推出新作品，都會上電台宣傳，在廣告時段用主打歌的旋律唱電台指定的宣傳詞。一般打歌期，歌手必須空出一個下午，一次錄三十個電台的分量，這工作幾乎沒人喜歡，但又不得不做。

有了數位分身就不一樣，只要複製好歌手的唱腔、聲調和旋律，然後直接讓AI唸電台指定的詞，就可以達成一樣的功效。如此一來，歌手可以省掉時間，完成不喜歡做的工作，廣播電台也不受影響，因為依舊是歌手的聲音；此外，分身甚至可以完成你無法親自執行的任務，比如電視製作人王偉忠，就透過分身創造一個英文和日文都非常流利的他（商業週刊1940期：高士閔，2025；3年內，AI代理人大爆發）。

C.2、數位分身的各種應用層面：

- 娛樂：數位分身可以用於娛樂，例如電腦遊戲、動畫和電影。
- 教育：數位分身可以用於教育，例如虛擬教學、模擬實驗和互動課程。
- 醫療：數位分身可以用於醫療，例如虛擬手術、醫學模擬和病人教育。
- 製造業：數位分身可以用於製造業，例如虛擬產品設計、模擬生產和品質控管。



C.3、數位分身的優點：

- 提高效率：數位分身可以提高效率，減少時間和成本。
- 提高安全性：數位分身可以提高安全性，減少風險和危害。
- 提高靈活性：數位分身可以提高靈活性，允許使用者進行多種模擬和互動。
- 提高真實性：數位分身可以提高真實性，提供更真實的模擬和互動體驗。

C.4、數位分身的挑戰：

- 技術限制：數位分身需要先進的技術和硬體支援。
- 成本：數位分身需要大量的資源和投資。
- 安全性：數位分身需要確保安全性和隱私保護。
- 資訊倫理：數位分身需要考慮倫理和道德問題。



D.1、網路零信任（Zero Trust）

什麼是零信任？就像公司或學校的「智慧刷卡系統」，即使你穿著制服，是學校或公司的一員，每次進入時還是要「刷卡」；由於網路環境越來越複雜，造成網路上的資訊安全相關問題層出不窮，希望透過對任何資料存取皆採取永不信任且必須驗證的原則，達成不論在何時何地存取資料皆保證一致安全性之相關技術。

核心精神：「永不自動信任，持續驗證身分」的網路安全原則，適用於個人數位生活與組織的資安防護，即使對方在校園內或使用學校電腦亦然。



D.2、網路零信任 3 大關鍵原則：

- 驗證所有人：
如果好朋友借用你的手機玩遊戲，你會幫他設定一組帳號或密碼，要求輸入後才能使用，還是解鎖手機後直接給他？
→ 零信任要求：每次存取敏感資料都要重新確認身分。
（例如：就像上廁所，即使大家都互相認識，還是要「敲門」確認）
- 最小權限原則：
班級工作分配，只有負責開門的同學需要拿到教室鑰匙，其他人則不需要。
→ 只給予完成任務所需的最低權限。
（例如：就像鑰匙分配，打掃教室的同學不需要保管教室的鑰匙）
- 假設已被入侵：
在游泳池更衣室的置物櫃保管個人物品時，即使櫃子已經附有上鎖的功能，很多人也會「把錢包藏進鞋子裡」。
→ 時時刻刻對所有網路流量持續監控與檢查。
（例如：就像考試監考，不只看在教室應考的考生身分正確與否，還要看是否有作弊行為）

D.3、為什麼需要網路零信任？

傳統防護漏洞 vs. 現代威脅情境	
傳統思維（城堡護城河）	現代零信任（行動防護網）
「校內電腦＝安全」	校內Wi-Fi連線也要加密
密碼用生日好記	強制兩階段驗證（如：簡訊＋指紋）
直接開放檔案分享	每次存取檔案都需審核



D.4、網路零信任的應用層面：

- 教育機構應用：
學生個人資料保護，教師每次在下載成績時都必須獲得臨時權限授權。
- 個人設備防護：
手機／筆電日常使用時，採取「生物特徵＋密碼」雙重解鎖（如Face ID＋複雜密碼）。
- 遊戲與社群平台：
零信任機制，每次登入需手機確認。
- 物聯網（IoT）設備：
家庭智慧裝置安全，零信任部署採取「區域隔離」措施，攝影機網路與主要網路分離，避免駭客入侵。
- 醫療資料管理：
電子病歷存取控制，醫師只能在診間電腦存取患者資料。
- 金融交易安全：
網路銀行防詐騙，以行為模式辨識（分析滑鼠移動模式與打字節奏）來判斷是否有外力介入或受人操控。
- 跨國企業防護：
遠距辦公資安，採取持續驗證的VPN連線（每15分鐘重新確認身分）。

D.5、如何在校園中運用零信任概念

在校園中，可以透過以下方式理解和運用零信任的概念：

- 身分驗證：
在使用學校的電腦或網路時，學生需要使用自己的帳號和密碼登錄，這樣可以確保只有授權的學生才能使用資源。
- 訪問控制：
如果學生想要進入某個特定的實驗室或資源中心，必須先獲得老師的批准，這樣可以防止未經授權的人進入。
- 持續監控：
學校可以使用監控系統來檢查誰在使用電腦和網路，確保沒有不當使用的情況發生。



D.6、網路零信任的優勢與劣勢

- 安全性增強，破除信任邊界，即使是內部流量也需加密並驗證，並加上最小權限範圍授權。
- 架構彈性多元，混合式辦公支援與物聯網防護。
- 符合個人資料保護法相關規範。
- 實施技術門檻較高，人力需求增加。
- 使用者常反映驗證過多繁雜，擔心誤擋風險。

網路零信任不是否定人性，而是為數位世界的每次互動繫上安全帶，就像我們跳傘活動一樣，每次跳傘前準備要確實檢查所有裝備，既是保護自己，也是尊重他人。



2-2 延伸學習

- 科勝科技(2023年8月18日)；【數位學生真實應用場景】數位學生+AI視覺辨識技術讓巡檢與資產管理更智慧化、更省時省力，取自：<https://youtu.be/8Sab3y50r2k>
- 非凡新聞台(2024年12月12日)；AI數位分身TheKeeper亮相！科科科技提倡合法授權創造價值 提供風險防範解決方案 | 非凡財經新聞 | 20241212，取自：<https://youtu.be/4w7L1cDxMpl>
- 中華電信研究院 | 科技新知；交通數位分身及AI號控最佳化解決方案，取自：https://www.chttl.com.tw/_news/n_tech20.html
- 密碼強度測試網站：<https://howsecureismypassword.net/>

◆ 問題一：數位身分的風險

許多網站提供「使用Google帳號登入」或「使用Facebook帳號登入」的功能，請說明這種單一登入(Single Sign-On)方式可能帶來哪些隱私或安全風險？

參考答案：

許多網站提供「使用Google帳號登入」或「使用Facebook帳號登入」的單一登入（Single Sign-On，SSO）功能，雖然大幅方便用戶省去重複註冊與記憶多組密碼的麻煩，但這種方式也帶來一些隱私與安全風險：

(1) 隱私風險：

- 資料共享：資料集中與濫用風險

使用第三方帳號登入可能會將大量個人資料授權給第三方應用程式或網站，包含姓名、聯絡方式、朋友列表等。這種資料分享若管理不善或遭到濫用，會導致個資外洩或隱私被侵犯。

- 集中風險：集中風險增加攻擊面

使用Google或Facebook帳號登入等SSO方式，代表這些大型數位身份服務供應商成為使用者的「數位身份中樞」。如果這些帳號被駭客入侵，駭客便可能取得使用者在其他所有第三方網站的存取權限，造成多個服務同時遭受威脅。

- 資料追蹤：跨平台追蹤與行為分析

透過SSO，服務提供商可能跟蹤用戶在不同網站的活動，進行行為分析或廣告定位，增加用戶的隱私疑慮。

(2) 安全風險：

- 帳號停用風險：中心化服務的潛在單點故障

當Google或Facebook等主帳號遭禁止、停用或服務中斷，用戶可能無法再登入所有綁定此身份的第三方服務，影響使用權利與體驗。

- 權限濫用：授權過度問題

用戶在使用SSO登入時，往往會被要求授權應用程式存取多種權限，部分權限可能超出使用需求，導致多餘資料暴露，增加個資風險。

- 單點故障：漏洞與資安事件風險

曾有駭客利用Facebook系統漏洞取得數位金鑰，藉此入侵數百萬用戶帳號及其第三方應用權限，暴露大量敏感資訊。

(3) 建議做法：

- 檢視授權給第三方的權限範圍。
- 定期檢查並移除不再使用的授權。
- 為主帳號啟用雙因子認證。
- 重要服務仍使用獨立帳號密碼。

結論：

雖然SSO提升了便利性與使用體驗，但使用時應謹慎審核第三方應用權限，啟用雙因子認證（MFA）加強主帳號安全，定期檢查與移除不再使用的第三方連結，才能有效降低隱私與安全風險。

◆ 問題二：網路零信任

零信任架構強調「最小權限原則」（Principle of Least Privilege）。

情境題：假設你是班上的班級鑰匙管理員，班上某位同學需要拿取班級儲物櫃的東西。請說明，你會如何應用最小權限原則來設定他的存取權限？

參考答案：

零信任架構中的「最小權限原則」意思是指每個使用者或實體（如裝置）在任何情況下，只被授予完成其工作所需的最低限度權限，避免多餘的存取權限造成安全風險。

以你是班上鑰匙管理員，班上同學要拿取班級儲物櫃物品為例，應用最小權限原則時，應用最小權限原則的做法如下：需要考慮「誰」、「什麼時候」、「在哪裡」、「做什麼」、「如何監督」等面向。

(1) 限定存取範圍：

只允許該同學拿取其「需要使用」的儲物櫃，不給予其他儲物櫃的鑰匙或存取權限。

(2) 限定存取時間：

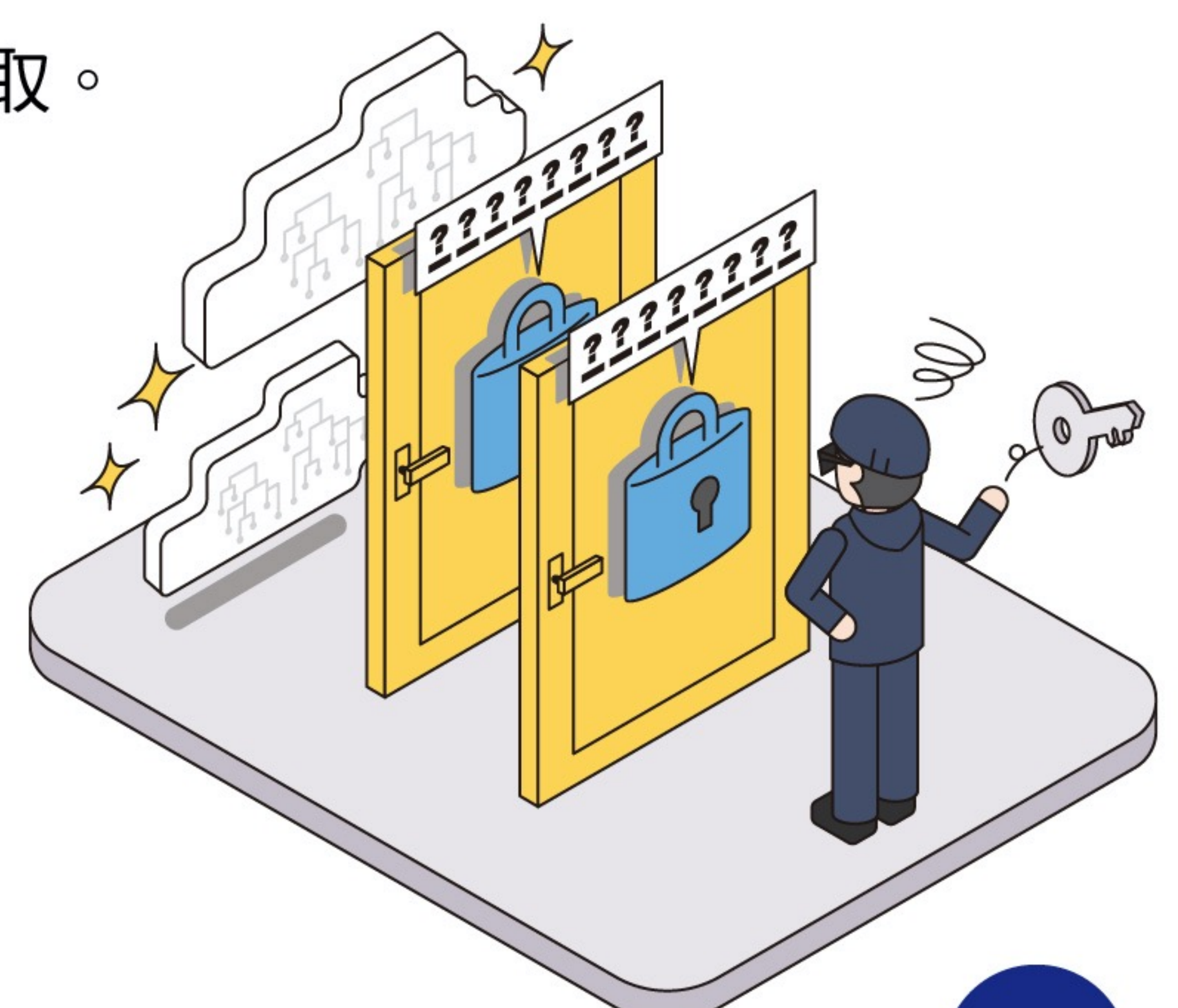
設定同學只能在特定時間段（例如上課結束後）存取，不允許無限制全天候存取。

(3) 審核身份：

在交付鑰匙前，確認同學的身份，避免未經授權的其他人拿取。

(4) 監控與紀錄：

建立鑰匙借用和歸還的紀錄，以備後續查核，防止濫用。



- 最差的做法（違反最小權限原則）

以下做法都是錯誤示範：

- ✗ 直接把鑰匙借給他，讓他自己去拿→無法確保他只拿自己的東西。
- ✗ 把鑰匙借給他一整天，放學再還→時間過長，可能被轉借他人或遺失。
- ✗ 給他萬用鑰匙，可以開所有櫃子→權限過大，可能侵犯其他同學隱私。
- ✗ 沒有登記借用記錄→無法追蹤責任，發生問題時無從查起。
- ✗ 讓他影印一把鑰匙給自己用→鑰匙數量失控，無法管理。
- ✗ 不確認身分就借出→可能是冒充的，或非本班同學。

- 與資訊安全的對應關係：這個班級鑰匙管理情境，對應到資訊系統的權限管理

班級情境	資訊系統對應
班級鑰匙管理員	系統管理員（Admin）
需要拿東西的同學	一般使用者
儲物櫃	資料庫 / 檔案系統
個人櫃子	個人資料夾
班級公物櫃	共享資料夾
鑰匙	帳號密碼 / 存取權限
借用登記簿	系統存取日誌（Log）
陪同開鎖	管理員權限提升
異常借用行為	異常登入偵測

結論：

- 只給需要的權限：夠用就好，不多給。
- 限定時間範圍：用完立刻收回權限。
- 限定存取範圍：只能碰自己的，不能碰別人的。
- 全程記錄監督：留下痕跡，可追溯責任。
- 定期檢視調整：需求改變時，權限也要跟著調整。
- 最佳做法：

當同學需要拿東西時，我會親自陪同前往，協助開鎖，確認他只拿取自己的物品後，立即上鎖並記錄，這樣既能滿足他的需求，又能確保班級財物和其他同學物品的安全。

最小權限原則的核心精神，簡言之，就是「給你完成工作所需的剛好足夠權限，沒有額外多餘的」，並且持續驗證和控制，這樣可以有效降低資安風險。

Q1

如果你的手機有一個「數位分身」，你希望它幫你做什麼呢？（例如：自動寫作業、提醒你考試範圍、推薦下課吃什麼點心……）

Q2

你希望分身「完全像你」還是「比你更完美」？為什麼？

Q3

醫療緊急狀況下是否應暫停網路零信任機制？



英文參考資料

- Vohra, M. (2022). Digital Twin Technology: Fundamentals and Applications (ISBN: 978-1-119-842-31-6). Wiley. Jenkin, T. (2023, March). What Is a Digital Twin and What Value Can It Bring to Your Organisation? Mesh-Ai.；民國114年2月20日，
取自：<https://www.mesh-ai.com/blog-posts/what-is-a-digital-twin-and-what-value-can-it-bring-to-your-organisation>
- Ankitha, V. (2025, January 20). The Role of Digital Twin Technology in Smart Cities Development. Toobler.；民國114年2月20日，
取自：<https://www.toobler.com/blog/digital-twins-in-smart-cities>
- Tor-morten, G. (2020). Digital Identities for Internet of Things Devices. IEEE, 2019 IEEE Conference on e-Learning, e-Management&e-Services (IC3e).；民國114年2月20日，
取自：<https://doi.org/10.1109/IC3e47558.2019.8971779>
- Elastic (Ed.). (n.d.). What Is Zero Trust? Elastic. <https://www.elastic.co/cn/what-is/zero-trust>
- Brook, C. (2024, October 23). Understanding the Zero Trust Security Model to Safeguard Digital Infrastructure. Digitalguardian. <https://www.digitalguardian.com/blog/understanding-zero-trust-security-model-safeguard-digital-infrastructure>



中文參考資料

- Microsoft Learn (2024/7/5)身分識別和存取權管理（IAM）基本概念；民國114年02月20日，
取自：<https://learn.microsoft.com/zh-tw/entra/fundamentals/identity-fundamental-concepts>
- 《商業周刊》3年內，AI代理人大爆發 撰文者：高士閔 (2025/01/16)技嘉科技. (n.d.). 數位分身.
[網路詞彙解釋]. 技嘉科技網站；民國114年2月20日，
取自：<https://www.gigabyte.com/tw/Glossary/digital-twin>
- 陳侑成 (2021, 12月8日). 製造業數位分身發展現況與應用趨勢；民國114年03月06日，
取自：https://www.moea.gov.tw/MNS/doit/industrytech/IndustryTech.aspx?menu_id=13545&it_id=395
- 國家資通安全研究院(2024/11/12) 零信任架構(ZTA)，民國114年03月06日，
取自：https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/ZTA/
- 香港網路安全事故協調中心 (Ed.). (2022, June 7). 資訊保安烏托邦由「零信任」架構開始. 香港網路安全事故協調中心；民國114年02月20日，
取自：<https://www.hkcert.org/tc/blog/information-security-utopia-starts-with-zero-trust-architecture>
- 晟威科技 (Ed.). (2024, August 27). 認識零信任（Zero Trust）－概念、原則與優缺點. 晟威科技；
民國114年03月06日，取自：<https://www.neway.com.tw/article-detail/zero-trust/>
- Paloalto (Ed.). (n.d.). 什麼是零信任架構. Paloalto.
<https://www.paloaltonetworks.tw/cyberpedia/what-is-a-zero-trust-architecture>
- Authme (Ed.). (2024, April 27). 什麼是零信任？如何實施零信任網路架構（ZTA）？. Authme.
https://authme.com/zh_tw/blog-ch/introducing-zero-trust/
- Pan, J. (2023, January 31). 永不信任，一律驗證：零信任（Zero Trust）概念與實作指引.
FREEDOM. <https://www.freedom.net.tw/tech-blog/zero-trust-guideline.html>
- Tenten (Ed.). (2023, December 16). 解密零信任 (Zero Trust)：基本原則與核心概念. LinkedIn.
<https://cn.linkedin.com/pulse/%E8%A7%A3%E5%AF%86%E9%9B%B6%E4%BF%A1%E4%BB%BB-zero-trust%E5%9F%BA%E6%9C%AC%E5%8E%9F%E5%89%87%E8%88%87%E6%A0%B8%E5%BF%83%E6%A6%82%E5%BF%B5-tentenco-6adv>
- Li, C. (2023, January 31). 零信任架構應用系統設計導論. Linked.
<https://cn.linkedin.com/pulse/%E9%9B%B6%E4%BF%A1%E4%BB%BB%E6%9E%B6%E6%A7%8B%E6%87%89%E7%94%A8%E7%B3%BB%E7%B5%B1%E8%A8%AD%E8%A8%88%E5%B0%8E%E8-%AB%96-ching-pei-li>

資訊素養與倫理 國中 5 版

出版 / 臺北市政府教育局

召集人 / 湯志民 臺北市政府教育局局長

副召集人 / 卓育欣 臺北市政府教育局資訊教育科科长

楊啓明 臺北市立明德國民中學校長

指導委員 / 賴阿福 臺北市立大學教授

盧東華 臺北市立大學助理教授

諮詢委員 / 林裕勝 臺北市文山區永建國民小學校長

曾文龍 臺北市立育成高級中學校長

陳玫良 臺北市立北投國民中學校長

總編輯 / 黃耀祺 臺北市立明德國民中學教務主任

編審委員 / 邱森德 臺北市立北投國民中學主任

洪瑞甫 臺北市立龍山國民中學主任

林國星 臺北市立明德國民中學教師

陳柏亨 臺北市立北安國民中學主任

陳好蓁 臺北市立明德國民中學教師

陳俊宏 臺北市立明德國民中學教師

郭怡君 臺北市立明湖國民中學教師

葛允文 臺北市立明德國民中學資訊組長

(按姓氏筆畫排列)

承辦單位 / 臺北市立明德國民中學

出版日期 / 中華民國114年9月

虛擬世界任遨遊

數位安全零信任，科技生活不設限



臺北市政府教育局

DEPARTMENT OF EDUCATION
TAIPEI CITY GOVERNMENT