數位環境中的兒少保護：從福祉觀點看數位風險與制度挑戰

陳威宇*
陳乘斌**

壹、兒少數位生活中的科技便利與潛在風險

當代兒少與青少年在快速數位化的時代中成長，數位科技已深刻融入他們的日常生活，成為學習、娛樂、社交互動與獲取資訊的重要途徑。這些便利與機會也伴隨著不斷變化的風險，包括隱私洩漏、網路霸凌、過度使用，以及數位性暴力與網路犯罪等新興危害。隨著人工智慧與沉浸式技術的發展，這些風險更趨複雜，對兒少的身心健康與整體發展構成嚴峻挑戰。面對此一現象，亟需採取跨部門、全社會的合作行動，結合有效的監管措施、安全導向的技術設計與全面的數位素養教育，並確保兒少的聲音能在政策制定過程中被真實聽見與重視（OECD, 2021；UNCRC, 2021；OECD, 2025）。

數位媒體的普及率極高，兒少與青少年幾乎隨時都可能接觸並使用網路。透過智慧型手機、平板與電腦，他們使用各類線上平台進行學習、創作、娛樂與社交，並在數位環境中獲取豐富的知識與表達自我的機會。這些數位媒介不僅促進同儕互動與社群連結，也讓兒少能參與公共議題、表達觀點，甚至在面臨心理困擾或需要特殊健康與社會資源時，獲得關鍵的支持與資訊。對於部分弱勢或難以被察覺需求的兒少，數位空間更是尋求協助、理解自我與建立認同的重要管道。然而，若缺乏足夠的媒體素養與安全意識，過度或不當使用仍可能帶來心理壓力、網路霸凌與隱私外洩等風險，這凸顯培養安全、負責任且具韌性的數位使用能力的重要性（Park, E. and Kwon, M., 2018；OECD, 2021；UNCRC, 2021；Laffier, Rehman, and Westley, 2025；OECD, 2025）。

數位化轉型雖為兒少福祉帶來新的機會，但同時也伴隨多種風險，我們可以依循「4C」框架來分類：Content（內容）、Contact（接觸）、Conduct（行為）與Contract（契約）風險（Livingstone and Stoilova, 2021）。其中，接觸與行為風險與數位性暴力及網路犯罪尤其密切相關，兒少可能接觸不適當或有害內容、與陌生人或潛在危險對象互動、遭受不當行為，甚至在缺乏保護的情況下參與不公

*本文作者係財團法人台灣兒童暨家庭扶助基金會社會工作處研發組資深專員
**本文作者係財團法人台灣兒童暨家庭扶助基金會社會工作處處長

平或具有風險的線上合約與交易。在這些風險中，兒少性剝削和虐待仍是線上環境中最嚴重的威脅，其規模、嚴重性及複雜性持續增加（OECD, 2023）。加害者可能透過線上互動建立信任，誘導兒少提供個人資訊或進行危險行為，進而實施性勒索或其他形式的剝削。生成式人工智慧（Generative AI, Gen-AI）進一步加劇這些威脅，例如AI生成的深度偽造（deepfakes）能製作高度逼真的兒少性虐待材料（CSAM），增加執法鑑識難度；並可能被用於性勒索或欺凌。同時，AI系統收集的大量數據可能遭到濫用，危及兒少隱私，且AI生成的資訊可能包含誤導或虛假內容，削弱兒少的判斷力與批判思維。儘管AI在教育與福祉領域具有潛力，其潛在風險仍需透過跨部門監管，技術安全設計以及媒體素養教育加以管控，以保障兒少在數位環境中的安全與福祉（UNODC, 2016；Dignum, V. 等人, 2021；OECD, 2021；UNCRC, 2021；Leaver and Srdarov, 2025；OECD, 2025）。

為了在數位時代提升兒少福祉，必須對數位環境的益處與風險有全面的理解，以整體策略促進各領域合作，形成共同責任，讓保護兒少的任務得以被社會各方一齊接住（OECD, 2021；OHCHR, 2021；Dirwan and Thévenon, 2023；OECD, 2025）。在規劃數位環境的保護與管理措施時，除了強化法律、政策與技術防護外，也必須將兒少與青少年的觀點與使用經驗納入政策設計與討論，持續傾聽他們的困難、期待與需求，唯有如此，政策與措施才能兼顧保護與尊重兒少權利，方能具備可行性。這不僅包括學校、家庭或社會層面的教育與引導，也需要將兒少的觀點納入科技設計、平台管理和政策規範中，使整個數位環境更符合兒少的真實需求（OECD, 2021；OHCHR, 2021；Third and Moody, 2021；UNICEF, 2024；OECD, 2025）。如同兒少的遊樂場一般，我們應體認到數位環境在設計與管理上必須兼顧安全；就像兒少遊樂場在設施規劃、使用流程與監管上需要考慮安全因素，數位空間也應透過「安全設計」（Safety by Design）原則與制度保障，提供兒少自由探索、學習與娛樂的機會，同時降低潛在風險，這將要求科技企業、平台運營者與政府共同承擔責任，打造安全且友善的數位環境，建立可持續的保護措施，結合教育與引導幫助兒少逐步培養識別風險、保護自身的能力（OECD, 2021；OHCHR, 2021；Dirwan and Thévenon, 2023；OECD, 2024；UNICEF, 2024；OECD, 2025）。這樣多層次的策略建構，兒少才能享有探索與使用數位資源的自由，也能在安全保障下健康成長，以兒少為中心，讓數位政策實現保護與賦權並重的目標。

貳、數位生活中的兒少福祉

經濟合作與發展組織（Organisation for Economic Co-operation and Development，以下簡稱OECD）於2011年透過「美好生活倡議」（Better Life Initiative）首次提出福祉框架，突破僅以經濟指標衡量社會進步的思維，改以多維度方式整合人們生活的客觀條件與主觀感受，強調「以人為本」的原則。此框架指出，個人福祉不僅取決於收入、教育、居

住等物質條件，也深受心理健康、社會關係與個人意義感等非物質因素的影響。

隨著數位科技深刻影響人們的日常生活，OECD進一步將「福祉」概念延伸至數位世界中的「數位福祉」（digital well-being），以探討科技使用對個人與社會幸福的多面影響。數位福祉的核心在於如何在科技帶來的學習、溝通與創新機會與其潛在風險之間取得平衡。對兒少與青少年而言，這不僅關乎教育與數位參與機會的拓展，更涉及心理安全、隱私保護與人際互動品質的維持（OECD, 2019；UNICEF, 2024；Laffier, J., Rehman, A. and Westley, M., 2025；OECD, 2025）。

為回應數位時代新興挑戰，OECD提出「數位福祉輪」（Digital Well-being Wheel），以評估各國在數位化機遇與風險治理上的表現。該框架涵蓋11個面向與33項指標，並將「數位安全」、「心理健康」與「數位素養」視為數位時代福祉的三大核心要素。這三者相互支撐；唯有在確保安全與促進心理健康的基礎上，透過素養培力，方能建立包容且永續的數位生態。對兒少而言，這樣的架構提供了政策與制度層面的保護方向，有助於防止數位暴力、強化自主能力，並促進其在數位社會中的安全與尊嚴（OECD, 2019）。

其中，「數位安全」是防範兒少數位性暴力與其他網路侵害的首要條件。OECD將數位安全定義為「為促進經濟與社會繁榮而管理數位安全風險的一系列措施」，並強調其不僅是技術性保護，更涉及倫理與社會責任，即是在保障兒少隱私、尊嚴與權益的同時，維持社會對數位服務的信任；例如，當網路上或數位平台出現個資外洩、影像濫用或性剝削內容時，不僅削弱兒少與家長對網路的信任，也直接侵害兒少的隱私權與人格尊嚴（OECD, 2019）。

在此安全保障的基礎上，心理健康構成兒少數位福祉的另一核心支柱。許多研究提到兒少過度使用網路或社群媒體與焦慮、憂鬱及睡眠問題相關，若是兒少遭遇數位性暴力，心理困擾將更加劇烈，可能引發創傷反應、孤立感與對他人的信任破裂（OECD, 2019）。不過，OECD與《兒少權利公約》第25號一般性意見都強調，兒少在數位環境中享有安全使用科技的權利，並指出若數位技術運用得當，仍可成為心理支持的工具，例如同儕支持社群，或是協助受害者重建自我效能感與社會連結。在兒少數位心理健康的核心策略中，並非防止過度使用，數位福祉應著重建立支援性、非剝削性的數位環境，使兒少能在尊重其權利的前提下，自主使用數位資源，安全參與學習、社交與創造活動，同時獲得必要的心理與情感支持。

此外，數位素養則是預防兒少數位性暴力與增強數位福祉的關鍵能力。透過技術、認知與情感技能的培養，兒少不僅能辨識網路風險、保護個人資料，也能更有效地尋求支援、建立安全的線上社交網絡。OECD將數位素養視為結合資訊判讀、隱私保護與情緒調節等能力的綜合素養，缺乏素養不僅造成「數位鴻溝」，兒少難以辨識風險訊號、保護自身資料或應對網路騷擾，也使兒少更容易受到線上侵害；相對地，具備良好素養的兒少更能主動管理線上行為、參與社群並維護自身安全。OECD建議，政府與教育體系應

將數位素養納入核心課程，推動學校與家庭共構安全且具韌性的數位文化，使兒少在受保護的環境中學習使用科技、理解界限並培養自我防護能力（OECD, 2019）。

綜上所述，數位福祉（digital well-being）是兒少在數位時代安全、健康且能自主使用科技的前提。OECD提出的數位福祉框架指出，保障兒少權益需要從三大核心面向著手：數位安全、心理健康與數位素養；數位安全確保兒少免於數位性暴力與其他網路侵害，維護其隱私與尊嚴；心理健康則強調創建支援性、非剝削性的環境，使兒少能安全參與學習、社交與創造活動；數位素養則提供實務技能與認知能力，使兒少能辨識風險、保護自身資料並積極管理線上行為。三者相互結合，為兒少在數位社會中創造安全、尊嚴與自主的發展條件，並為政策與教育實踐提供指引，推動包容、韌性與永續的數位生態。

參、兒少數位風險現況

數位科技的普及使兒少與青少年在網路環境中面臨的風險日益多樣且複雜，特別是「接觸風險」（contact risks）與「行為風險」（conduct risks）的急劇增加。其中，數位性暴力與兒少性影像犯罪已成為最受關注的議題之一（Livingstone and Stoilova, 2021；OECD, 2021）。根據衛生福利部統計，2024年臺灣通報的「兒少及少年性剝削」案件共3,582件，較2023年增加228件，顯示案件數持續增長。通報中以「拍攝、製造、散布、播送或交付兒少或少年性影像」3,104件，約占86.7%，為最多見的態樣，凸顯性影像犯罪的嚴重性；同時，約11.1%的受害者為12歲以下兒少，也反映受害者年齡下降的傾向，顯示兒少在更年幼的時候即面臨數位性風險。

一、兒少網路性風險與性影像犯罪

根據WeProtect Global Alliance（2023）的全球研究，網路性傷害（online sexual harms）在兒少中相當普遍；約54%的18至20歲年輕人表示，18歲之前曾遭遇網路性傷害，其中女孩（57%）比男孩（48%）更易成為受害者，而性別少數族群及身心障礙青少年面臨更高風險；調查也顯示，首次接觸露骨性內容的平均年齡呈下降趨勢，18歲受訪者的平均首次接觸年齡為12.7歲。

在台灣，自2017年起，兒少性剝削案件通報人數逐年增加，自2017年的1,060人次增至2022年約2,280人次，2023年性別三法修法及「妨害性隱私及不實性影像罪」實施後，2024年通報人數達3,582人次。統計顯示，雖然被害人仍以國中生和高中職生為主，但國小生受害人數也顯著上升，從2017年的80人增加至2024年約224人，增幅約2.8倍。近年來，性影像犯罪已成為兒少性剝削案件的主要型態，從2017年的52%上升至2024年的87%，其中大多數案件涉及「拍攝或製造兒少進行性交或猥褻行為的影像」，且高達46%的散布影像來源為兒少自拍。同時，性勒索（sextortion）案件威脅正持續增加，犯罪者利用受害者的性資訊或影像進行勒索，要求提供更多影像或金錢，反映兒少面臨的網路性風險日益複雜（衛生福利部，2025；內政

部警政署，2025）。

二、網路誘騙與跨平台勒索

由於經驗與判斷力有限，兒少與青少年容易成為網路性剝削、數位勒索及在線欺詐的目標。犯罪者常利用網路科技與兒少建立關係，進而實施剝削或侵害。他們會收集兒少的個人資訊、興趣與弱點，假裝有共同興趣或相似背景，在社交媒體、線上遊戲與通訊平台上，透過心理操縱與誘騙手段接近兒少。網路誘騙（Grooming）是其常見手法，涉及「4C」框架中的「接觸風險」（Livingstone and Stoilova, 2021；OECD, 2021；OHCHR, 2021；OECD, 2023；WeProtect Global Alliance, 2023；OECD, 2024；Protect Children, 2024；UNICEF, 2024；OECD, 2025）。犯罪者在選擇受害者時，會評估目標的吸引力、是否容易接觸以及是否展現脆弱性；鎖定經常使用隱私設定寬鬆的平台或在網路上流露孤獨與被忽視感的兒少。接著，他們透過聯繫受害者建立信任，從網路管道蒐集資訊，假裝與受害者有共同興趣愛好和相似家庭社會背景，藉此接近、建立融洽關係並贏得信任。建立信任後，犯罪者會將友誼發展成排他性且保密的關係，進一步孤立兒少，並可能詢問受害者帳戶是否受父母或其他人員監控，以評估被發現風險（Livingstone and Stoilova, 2021；OECD, 2021；OECD, 2024；Protect Children, 2024）。

犯罪者還會利用跨平台轉移策略，即所謂的「Off-platforming」，先在兒少流行的平台，諸如社交媒體或線上遊戲，建立初次接觸，隨後誘騙受害者轉移至審核較少或端到端加密的通訊服務，在這些私人空間中，犯罪證據難以被識別或獲取（Protect Children, 2024）。這種轉移往往伴隨著數位勒索（Sextortion），即犯罪者利用已取得的性資訊或圖像，持續勒索更多性材料、強迫線下性接觸，或索取金錢以換取不公開分享。一旦掌握性影像，他們便威脅受害者提供更多內容，甚至強迫兒少對自己或同儕實施性暴力，或錄製、直播虐待行為。若影像被上傳至網路、雲端或私人論壇，將可能被反覆下載與分享，造成持續傷害且難以徹底清除。最終在於達成性剝削、性虐待或財務勒索之目的（OECD, 2021；Protect Children, 2024）。

三、AI與Deepfake對兒少的威脅

人工智慧（AI）與深度偽造（Deepfake）技術的快速發展，兒少在數位環境面臨更多樣的受害風險。生成式AI和深度偽造技術降低創建和傳播高度逼真內容的門檻，使犯罪者能製作虛假的圖像或影片，冒充他人或將兒少的肖像合成至不當內容之中，用於欺凌、剝削甚至性勒索。國際報告指出，Deepfake影片數量曾出現大幅增長，其中大部分為色情內容，而這類影片也可能被用於性勒索（sextortion）行為，進一步增加青少年的心理壓力與自殺風險（Metz, 2019；Ajder等人, 2019；台灣網路資訊中心，2020；法務部，2021）。此外，AI生成的兒少性虐待材料（CSAM）也讓執法部門難以辨別真偽，帶來新興的法治、調查與防治挑戰（Interpol, 2024；OECD, 2024）。

AI帶來的風險不僅限於深度偽造。在社交媒體平台上，AI驅動的推薦演算法可能放大

兒少接觸不適當內容的可能性，影響他們的心理健康。例如，演算法透過濾鏡和精選內容推廣不切實際的身體標準，容易引發焦慮、自我認知偏差、抑鬱、社交退縮，甚至增加自傷或不道德行為的風險。此外，AI系統收集的個人數據可能被濫用，損害兒少的隱私與安全；深度偽造內容也可能被用於網路欺凌，對兒少造成心理傷害（UNICEF, 2020；OECD, 2021；UNICEF, 2023；OECD, 2024）。

面對AI帶來的新型風險，建立健全的監管與安全設計成為必要措施。數位服務提供者應將保護兒少的設計原則嵌入產品和服務中，例如設定默認隱私權限、提供內容篩選功能，以及限制數據使用於必要服務範圍。聯合國兒少權利委員會建議，禁止利用兒少的數位特徵進行商業分析或定位，以保障其數據不被濫用。同時，制定年齡保證機制和相關標準，幫助服務提供者評估兒少特有的風險並採取適當保護措施，也對提升兒少的數位安全至關重要（UNICEF, 2020；OECD, 2021；OHCHR, 2021；UNICEF, 2023；Interpol, 2024；OECD, 2024）。

國內外數據顯示兒少性影像犯罪與性勒索案件持續上升，受害者年齡逐漸下降，顯示網路誘騙與跨平台勒索等行為日益猖獗，造成兒少長期心理壓力與受害。AI與深度偽造技術雖展現科技進步，卻同時放大這些風險，降低製作與散布虛假或剝削性影像的門檻，並透過演算法推播造成兒少心理負擔與隱私威脅。因此，兒少的安全與福祉須從科技技術設計、教育引導與法律監管三方面同步加強：數位平台應落實預設隱私保護與內容過濾，政府與產業需建立嚴謹的監管機制，並透過教育提升兒少與家長的數位安全意識，以共同減輕AI時代帶來的潛在危害。

肆、家扶調查看見：兒少數位性暴力風險現況與保護缺口

根據2024年臺灣衛生福利部的官方統計，兒少性剝削被害者中，年齡層為12歲至未滿15歲的國中前兒少，約佔性剝削被害人的46%，為受害人數最多的群體。這顯示國中前的兒少已面臨較高的性剝削風險，也反映出性剝削受害者呈現低齡化趨勢。其後依序為15歲至未滿18歲的青少年及未滿12歲的兒少，顯示兒少在早期階段即暴露於性剝削及數位性風險之下。

家扶基金會針對台灣兒少於2023至2025年間進行的《網路性剝削情境風險辨識調查》、《兒少網路社群使用習慣調查》以及《兒少數位足跡調查》進一步揭示了低齡兒少面臨的數位危險情境。

一、低齡兒少網路風險與安全意識的迫切課題

調查看見，接受調查的小學中高年級學生，已可能面臨提供私密照片、網路霸凌及購物詐騙的風險。在私密照外流方面，約有1.1%的兒少自述曾提供個人私密照片。此外，兒少對於「以愛為名」的誘騙手法辨識能力較低，這類情境通常涉及要求兒少提供私密照片以證明感情，是兒少最難察覺的陷阱；曾遭遇類似情境的兒少中，有21.7%會選

擇配合答應。同時，網路上露骨內容的接觸也不容忽視，約有6.6%的兒少曾被傳送色情訊息而遭到騷擾，並且有超過兩成（21.4%）的兒少會主動點擊標示「未滿18歲」警語的頁面，顯示他們在網路環境中仍存在明顯的風險暴露。

鑑於有16.3%的兒少在6歲前就開始使用網路社群，且超過九成在升上國中前已接觸社群平台，相關數據亦顯示，不僅青少年，連國小高年級學生都可能成為數位性剝削與網路誘騙的目標。可見兒少在很早的階段便進入網路世界，也因此更容易遭遇潛在風險。這說明提升兒少的網路安全意識與自我保護能力，應從更早的年齡開始著手。由於這類風險往往具有隱蔽性與欺騙性，兒少在心理安全、隱私權保障，以及風險辨識與防範能力方面的需求，更凸顯出在數位環境中建立完善保護機制的迫切性。

二、兒少數位隱私缺口成性暴力誘騙目標風險

兒少在數位環境中的隱私設定，成為數位性暴力犯罪者鎖定目標的重要破口。犯罪者傾向選擇隱私設定較寬鬆的兒少，藉由其公開的個人資訊、興趣與社交互動作為誘騙素材，進一步建立信任並實施操控。這些資訊不僅讓犯罪者瞭解兒少的喜好和脆弱點，也成為設計網路誘騙手法的基礎（Livingstone and Stoilova, 2021；OECD, 2021；OECD, 2024；Protect Children, 2024）。

然而，調查顯示，兒少在數位安全與隱私設定方面仍存在顯著缺口。近半數兒少表示不知道如何使用社群媒體或網路平台的隱私設定，對「數位足跡」概念不熟悉，且許多兒少對個人資料的公開風險缺乏認知，例如生日、照片與姓名等可直接辨識身份的資訊仍被部分兒少公開。這些缺口不僅使兒少自身無法有效防護，也為犯罪者提供了誘騙的便利條件。

三、素養教育與使用陪伴的需求

社會經常將兒少保護責任僅只放在家庭上，作為學習安全與培養防護意識的重要防線，但家扶調查看見，家長在這方面的參與有限。約有四成三（43.52%）的家長並未特別關心兒少使用社群媒體的情形，近四成（38.49%）的兒少也表示家長從未與他們談過網路安全相關話題。此外，有36.5%的兒少指出，家中未曾教導如何辨識網路性剝削風險，而這些兒少在風險辨識測驗中的表現也相對較低。

儘管學校仍是兒少獲取網路安全知識的主要來源，但多數兒少認為，家人的陪伴與討論更能增強他們的安全感與防護意識。家扶的調查發現，當家中長輩會主動關心或討論兒少的社群使用時，其遭遇瀏覽色情內容或被傳送色情訊息的比例明顯較低，顯示家庭陪伴在預防網路風險中具有關鍵作用。

伍、家扶呼籲跨域共責：構建兒少數位安全與福祉的綜合防護

從文獻爬梳與調查數據分析可見，網路世界中的兒少保護並非單一層面的議題，而是一項橫跨教育、家庭與社會結構的綜合性挑

戰。為因應網路風險與數位性暴力等新興問題，應採取「全社會、多部門」的整合策略（Whole-of-society and multi-sectoral approach），政府、企業、學校、家庭及兒少本身共同分擔任務與責任，而非僅由個人或照顧者承擔（OECD, 2021；Dirwan and Thévenon, 2023；Holly等人，2023；UNICEF, 2024；OECD, 2024；OECD, 2025）。家扶基金會建議，唯有家庭、學校與社會共同參與，才能在數位環境中建立具實質防護力的兒少保護機制。

一、家長如何守護數位世界中的兒少

茫茫網路處處潛藏風險，從交友詐騙、性勒索到深度偽造影像，讓許多家庭與家長在面對兒少在網路世界活動時感到無力與不安。但在多層面的整合策略中，家庭仍是可以扮演兒少最直接且關鍵的防護網，父母與照顧者在引導兒少安全使用數位媒體的過程中，將扮演著無可取代的角色。唯有當父母被賦權、具備正確的資訊與工具，才能真正陪伴兒少在數位環境中安全成長。

家扶認為，建立信任與開放的雙向溝通關係是數位兒少保護的基礎。家長可以從理解兒少使用社群媒體的需求與感受開始，採取開放的態度，與兒少共同討論使用目的、體驗與感受，而非僅以禁止或監控作為主要手段。唯有在這樣的雙向溝通下，兒少在面臨網路風險或困擾時，才更可能主動求助與分享。調查顯示，當兒少在網路上遭遇帳號被盜、照片被轉發或個人秘密被公開等「貼文不當使用」情況時，仍有近七成會選擇向父母或家人傾訴，可見家庭信任關係是最有效的防護力量之一。建立信任與開放的雙向溝通關係，將提供家長持續關心兒少的網路使用情況機會，若察覺異常或兒少出現情緒困擾，就可以即時提供協助，並引導他們認識可求助的資源與管道，使兒少在遭遇風險時，始終能感受到家庭的支持與安全。

在雙向溝通的基礎上，家長可與兒少共同討論並制定明確的網路使用規範，例如不公開個人資料、不點擊含有「未滿18歲」警語的頁面等，使家庭守則成為具體且可行的安全基礎。同時，家長也能從明確制定的規範中，協助兒少培養健康的數位生活習慣。這些規範不應僵化，而應隨著兒少年齡與成熟度逐步調整，從嚴格監督過渡到給予青少年更大的自主管理空間；透過這些具體而靈活的做法，兒少能在安全框架下學習負責任的使用行為，逐步發展出良好的自我管理能力。

家長可以與兒少共同培養風險辨識能力與性別安全意識，自己先學習並陪伴兒少理解網路世界的優勢與風險，真誠討論網路誘騙、性勒索及假交友等議題，讓兒少學會辨識潛在危險。此外，我們需讓兒少明白「傳送私密影像」並非表達感情的工具，並說明影像外流可能造成的長期後果，以降低受害風險。除此之外，親子可透過共同參與數位活動，一起觀看教育性或互動性內容，促進家庭對話並提升數位素養。透過安排使用時間、內容選擇與互動方式，使科技成為親子連結與學習的媒介，而非潛在風險或衝突來源。

二、政府、平台與社會共責：打造兒少數位安全與防護體系

前述文獻指出，網路與社群平台、政府與

數位服務提供者應承擔確保兒少安全的責任。平台應以兒少能理解的語言說明個資蒐集與使用目的，提供明顯可見的求助與檢舉管道，讓兒少在遭遇威脅時能快速獲得支援。然而，目前仍有超過半數的兒少不知道如何設定隱私權限，顯示平台在介面設計與教育引導上仍有改進空間。為此，政府應強化立法與治理體系，保持法律與制度與時俱進，應對數位性剝削、AI深度偽造等新興犯罪，同時建立透明問責與投訴補救機制，並加強執法單位的數位工具與跨國合作能力。數位服務提供者則需推行「安全設計」，從產品與服務設計中嵌入保護措施，包括預設隱私設定、內容篩檢與AI檢測、年齡驗證、阻止成癮性功能，以及提供清晰可訪問的報告與投訴管道（OECD, 2021；OHCHR, 2021；UNICEF, 2024；OECD, 2024；Better Internet for Kids, 2025；OECD, 2025）。針對數位性暴力與兒少性剝削，平台應積極移除與阻斷不法資訊，保留證據供司法調查，並配合國際合作打擊犯罪供應鏈。最後，社會大眾需持續接受教育，瞭解散布、持有或製作兒少性剝削影像的嚴重性，自覺刪除、停止轉傳，形成全民防護的社會共識，並讓兒少瞭解可利用的正式求助管道，保障心理創傷修復與重建的支援。

家扶也呼籲社會可以以下行動回應數位風險下的兒少需求。首先，兒少的數位識讀教育應向下延伸至國小階段甚至學齡前，由於多數兒少在入小學前就已開始使用網路，素養教育應及早進行，並考慮將「數位足跡」、「隱私保護」與「網路誘騙辨識」等內容納入課程，培養面對不同情境與操控手法的辨識力。其次，家庭教育的角色必須被支持與重新強化，對於兒少反映從未於家中討論過網路安全議題，與反映此需求，政府與民間機構可以積極推動家長數位素養教育，協助家長理解兒少數位風險與保護意涵，並鼓勵家長主動與兒少討論網路交友、個資保護等主題，成為兒少最堅實的後盾，避免暴露於風險之中。

在數位風險高度滲透的時代，兒少網路安全是一項跨越家庭、教育與社會體系的共同責任，最有效的防護力量不僅來自制度與科技，更來自兒少的重要關係人及早參與、持續陪伴與信任關係的建立。唯有如此，兒少才能在數位社群中安心互動，避免遭受不當侵害，進而促進其整體數位福祉，保障心理安全、隱私、社交自主與健康使用網路的環境。將網路安全視為數位福祉的一部分，才能真正支持兒少在數位世界中健康、平衡且有韌性的成長。