

網上校管系統雲端服務先導計劃 2020

常見問題及答案

一般

1) 問：「網上校管系統雲端服務先導計劃」目的為何？這計劃如何推廣至其他學校？

答：為減輕學校教職員管理及支援網上校管系統伺服器方面的工作，以及加強系統保安，本局於 2018 年開始推行雲端服務先導計劃，試驗將現時由學校負責管理的網上校管系統伺服器，遷移至雲端平台。現時有 225 所學校已參加先導計劃，整體運作暢順，學校普遍滿意雲端平台各方面的表現。本局擬循序漸進地推行有關計劃，先於二零二零年增加約 150 個學校名額，以進一步完善具體操作安排，並初步計劃在隨後兩年安排其餘所有學校分批遷移至雲端平台。

2) 問：學校是否需要進行招標程序，自行招募承辦商提供雲端服務？

答：不需要。所有學校會使用同一承辦商提供的雲端平台服務。教育局已為上述服務進行中央招標程序，並已預留相關款項，支付雲端平台服務費用。

3) 問：「網上校管系統雲端服務先導計劃 2020」的擬定日程表為何？

推行計劃	擬定日程表
教育局向學校發出邀請信	2020 年 6 月 15 日
學校以傳真方式遞交「回條」至教育局	2020 年 6 月至 7 月(截止日期：7 月 8 日)
教育局通知學校名額分配的結果	2020 年 7 月下旬 / 8 月上旬
教育局舉辦簡介會，向獲分配名額的學校介紹相關詳情，包括數據遷移的具體安排及操作示範	2020 年 10 月
雲端平台完成最後測試	2020 年 10 月
學校將網上校管系統伺服器的數據遷移至雲端平台	2020 年 11 月至 12 月

系統資料遷移及儲存

4) 問：參加計劃的學校，將如何把數據遷移至雲端平台？整個數據遷移的過程需要多少人手和時間？

答：本局會為學校提供進行數據遷移所需的工作軟件和程序指引。根據過往的經驗，大部分學校的教職員（大約一至兩名）只需一至兩天的時間便可完成整個數據遷移及測試過程。

- 5) 問：承辦商的網絡能否同一時間為多間學校進行數據遷移？
答：教育局會於數據遷移期間，分批安排合適數量的學校遷移數據至雲端平台，以確保過程暢順。
- 6) 問：網上校管系統雲端服務分配給每所參加計劃的學校的儲存容量為多少？
答：每所參加計劃的學校將獲分配足夠的容量以儲存網上校管系統的資料庫。因應學校資料庫的實際大小，服務平台會適當地調整分配容量。
- 7) 問：哪些數據資料可遷移至雲端存放？
答：整個網上校管系統的數據資料及所有經網上校管系統處理的檔案庫將會被遷移至雲端存放，以確保所有系統功能運作如常。
- 8) 問：把網上校管系統伺服器數據遷移至雲端後，學校可否把現有伺服器作其他用途？
答：不可以。學校須保留現行的網上校管系統伺服器，以作後備之用。
- 9) 問：雲端平台的操作與現時有甚麼不同之處？雲端平台上的網上校管系統可支援多少用戶同時使用？
答：雲端平台的系統會於系統保安模組新增雲端服務管理頁面，以供用戶下載備份及更改遠端桌面視窗的密碼。除此之外，對用戶而言，網上校管系統提供的模組、功能、介面及工作流程及可支援用戶數目都沒有分別，學校用戶使用雲端平台上的網上校管系統所需的知識及技巧，與之前的版本並沒有分別。

資料保安及備份

- 10) 問：「網上校管系統雲端服務先導計劃」有甚麼保安措施？
答：雲端平台的保安措施包括：
- i. 承辦商及其數據中心必須遵守由政府資訊科技總監辦公室（OGCIO）制定的資訊科技保安指引。
 - ii. 數據中心會架設網絡防火牆，並每天 24 小時監測伺服器的運作情況。相關工作人員必須獲得認可才能進出數據中心。
 - iii. 承辦商已取得相關資訊安全管理的 ISO 認證。
 - iv. 採用私有雲模式，主要的硬件、軟件、網絡設備等都是專為此網上校管系統雲端服務而設，不會與其他系統的雲端服務共

用。

- v. 沿用網上校管系統三種工作站擁有不同登入權限的設計，網上校管系統雲端服務會分辨以下三種工作站：已連接虛擬私人網絡 (VPN) 的工作站、其他校內工作站、以及校外工作站，各有不同的登入權限。
- vi. 用戶連接 VPN 時必須擁有 VPN 帳戶及保安編碼器作雙重認證。

11) 問：雲端服務承辦商提供的保安編碼器有何用途？每所參加計劃的學校可獲分配多少保安編碼器？系統設計可否容許學校多名用戶同時進入雲端平台的網上校管系統 VPN 網絡？有甚麼系統功能必須連接 VPN 後才能使用？

答：每所參加計劃的學校將獲分配軟體及硬體保安編碼器各一，以供用戶比較相關操作安排。學校可使用雲端服務承辦商提供的保安編碼器，進入雲端平台的網上校管系統 VPN 網絡。任何電腦連接 VPN 後，便會獲得現時網上校管系統網絡內工作站的相同權限，可使用以下的系統功能：

- i. 「系統保安」模組內的「網絡協定位址設定」功能。
- ii. 用 Crystal Reports 修改報表範本後，以 ODBC 連接數據庫預覽結果。
- iii. 使用「系統保安」模組內新增的「雲端服務管理」頁面。

基於保安理由及 VPN 軟件版權問題，每個保安編碼器同一時間只供一名用戶進入雲端平台 VPN。

12) 問：在遷移至雲端平台後，學校是否需要自行購買安全通訊協定憑證(SSL Certificate)？

答：不需要。教育局將為所有學校購買安全通訊協定憑證。

13) 問：學校及學生資料儲存於雲端平台，是否安全？教育局及承辦商是否有權存取學校雲端平台內的資料？

答：所有上載到承辦商的資料均會被加密，並只有學校負責人擁有解密鑰匙，教育局及承辦商均不能查閱。

14) 問：參加計劃的學校，是否需要進行恆常的系統維護及資料備份工作？

答：教育局委託的承辦商將提供雲端服務，支援伺服器日常的維護工作，包括進行軟件更新，以及處理備份等。雲端平台將以中央模式處理網上校管系統的版本升級程序。雲端服務會於每天凌晨一時至上午六時暫停，進行系統維護和處理備份等工作。另外，學

校可因應個別需要而自行於雲端服務管理頁面下載資料庫作備份。

15) 問：經雲端平台處理的學校備份資料(包括整個虛擬機的備份影像及系統資料庫加密 zip 檔)，承辦商將會如何處理？有關備份資料會保存多久？

答：承辦商每晚會為系統進行備份，所有備份資料均會被加密，並只有學校負責人擁有解密密碼。上述備份資料在數據中心及另一備份中心均會保存一份拷貝。每晚的備份資料會保存一個月，而每月最後一日製作的備份資料，則會保存一年。在保存期後，所有備份會被新備份覆寫。

16) 問：學校可否下載於網上校管系統雲端平台上學校的備份資料？數據有否加密？

答：學校可以從網上校管系統雲端平台下載經過加密的學校數據，只有學校負責人擁有該解密鑰匙。

17) 問：雲端服務的系統保安有何特色及優點？

答：保安方面：

- i. 網絡保安架構及設定均符合政府資訊科技總監辦公室(OGCIO)高規格要求。
- ii. 經雲端平台處理的學校備份資料，均會保存一份拷貝資料在數據中心及另一備份中心，能確保備份資料安全地儲存。
- iii. 所有儲存在雲端平台的資料均會被加密，解密鑰匙由校方保管。教育局及承辦商均不能查閱。
- iv. 數據中心有嚴密的保安設施及指引，以保護系統儲存的資料。
- v. 虛擬機內不容許安裝或存放不相關的軟件或檔案及不開放 Windows 的遠端桌面服務(Remote Desktop Service)，以保持網上校管系統的穩定及安全。
- vi. 定期升級網上校管系統版本，緊貼最新版，減少系統可能出現的問題。

人力資源方面：

- i. 減省學校工作量，網上校管系統雲端服務會由教育局中央統籌並進行版本升級。
- ii. 減少人為設定錯誤而引起的問題。

維護方面：

- i. 由數據中心的專業人員負責系統管理及維護，定期更新系統軟件及監測系統的運作情況。

- ii. 若數據中心監測到不尋常狀況，數據中心人員會即時收到系統通知，並迅速應對及維護。
- iii. 數據中心內的環境維持在最適合電腦運作的溫度，電力供應穩定，以保持網上校管系統的運作暢順。

系統設定與日常操作

18) 問：在系統使用的高峰期（例如：考試入分期間），雲端平台服務是否能負荷不同學校眾多用家同時間使用系統？

答：在雲端平台上，各學校的伺服器均享有獨立資源。系統表現不會受多間學校同時使用所影響。教育局亦已對雲端平台系統進行負載模擬測試，例如測試單一學校多名用家同時使用、數十個虛擬伺服器同時運行等，結果顯示其系統效能與現時網上校管系統相若。此外，在各虛擬伺服器內的 Windows 操作系統及各系統軟件，已作了最佳化設定，以確保各學校的網上校管系統運作暢順。

19) 問：如何確定學校現行連接互聯網的頻寬是否能應付雲端服務的需求？伺服器數據傳輸大小是否有所限制？

答：學校現時連接互聯網的頻寬若有 100Mbps 便應足夠，最好確保當中有大約 10Mbps 頻寬預留給網上校管系統雲端服務使用。

20) 問：參加計劃後，學校是否仍可按照以往工序編修 Crystal Reports 範本？

答：安裝了 Crystal Reports 的工作站，須修改一次其 ODBC 設定，以連接至雲端平台上的網上校管系統數據庫。每次編修範本時，學校需要先使用保安編碼器連接 VPN 網絡，然後依照以往工序編修範本。

21) 問：雲端平台的網上校管系統伺服器可否安裝附加程式或外掛系統？

答：雲端平台將沿用網上校管系統一貫建議的安裝設定。除了用作修改報告範本的 Crystal Reports 程式外，其他任何程式或外掛系統均不可安裝及連接雲端平台的網上校管系統伺服器。

22) 問：雲端平台求助台的服務時間為何？現有的網上校管系統求助台熱線是否仍然適用？

答：雲端平台求助台開放時間跟每天網上校管系統雲端服務時間一致，即每天上午六時至翌日凌晨一時，為學校提供有關雲端服務的技術支援。現時網上校管系統求助台熱線的辦公時間和

服務範圍則維持不變。有關雲端伺服器及網絡的操作問題，學校可聯絡雲端平台求助台；有關網上校管系統的使用問題，現時網上校管系統求助台將繼續提供技術支援。

23) 問：參加計劃後，學校可否在有需要時自行重新啟動網上校管系統？

答：在數據遷移至雲端平台後，學校仍然可有需要透過新增的雲端服務管理頁面，或要求承辦商雲端服務求助台重新啟動網上校管系統。

24) 問：當局會否在每次雲端平台上的網上校管系統進行版本升級前預先通知學校？

答：每次網上校管系統版本升級均由中央統籌處理。在每次版本升級前，本局會經聯遞系統向學校發出有關版本升級的訊息，並通知學校有關安排和版本升級進行的確實時間。

25) 問：學校可否因應工作需要，提前安裝已發布的版本升級？

答：系統通常將設定於新版本升級發布後的第 14 個曆日，由中央統籌進行版本升級。學校亦可因應本身需要，於新增的雲端服務管理頁面，自行進行網上校管系統版本升級。

26) 問：如雲端平台的伺服器因故障未能提供服務，學校可以重啟校內的網上校管系統伺服器處理相關工作嗎？學校是否需要如常在原有的校內伺服器進行網上校管系統版本升級，以作後備之用？

答：基本上，承辦商已有足夠的服務承諾，確保網上校管系統雲端服務可暢順運作。假若雲端平台遇上特別事故而未能於短時間內恢復正常服務，學校可視乎需要，使用定期自行下載的資料庫備份，或安排向承辦商提取最新的資料庫備份，以啟動校內的網上校管系統伺服器，處理學校工作。資料庫備份檔已包含網上校管系統最新版本，學校無需定期在原有的校內伺服器進行網上校管系統版本升級。

27) 問：在遷移至雲端平台後，學校原有的網上校管系統伺服器、HTTP 伺服器和網上校管系統路由器是否需要繼續進行硬件保養？

答：校內原有的器材須保留作後備之用。學校不可將器材改作其他用途，並應定期安裝系統更新，包括網上校管系統伺服器的 Windows Updates、防毒軟件及病毒定義的更新、HTTP Server 的安全性和效能更新，網上校管系統路由器的 firmware update 等，以及繼續為相關硬件進行例行保養及維修。學校可繼續向教育

局申請伺服器的保養維修費用。

28) 問：學校可否同時使用校內的網上校管系統及網上校管系統雲端服務，直到網上校管系統雲端服務運作良好時，才停用校內的網上校管系統？

答：不可以。基於軟件版權問題，部份系統軟件同一時間只能在一部伺服器上運作。另外，聯遞系統有註冊機制，同一學校只有一台網上校管系統伺服器可與教育局連線交收資料。

29) 問：雲端平台上的 8 個虛擬機主機(VM Host)會為多少間學校提供服務？

答：8 個虛擬機主機可供 150 個虛擬機運作，每個虛擬機安裝一個網上校管系統。

其他

30) 問：雲端平台的數據中心位於何處？

答：雲端平台數據中心及其數據備份儲存中心均設於香港特別行政區境內。

31) 問：學校在參加「網上校管系統雲端服務先導計劃」後，是否可以退出此項計劃？

答：本局目前不會強迫學校參與上述計劃。本局與承辦商會作出妥善安排以確保此項計劃的服務質素。我們並會盡力作出協調以配合學校的整體需要。

32) 問：遷移至雲端平台後，網上校管系統會支援更多瀏覽器嗎？

答：網上校管系統現時主要支援 Internet Explorer 11 及 Chrome。