致： 全體學系系主任、學院院長及部門主管
全體教職員及同學

個人資料的管理及保安

引言

1. 個人私隱的範圍非常廣闊，而個人資料私隱是其中十分重要的一環，受到《個人資料（私隱）條例》的保障。所有存於紀錄，令我們能夠清楚確認一個在世人士的身份之資料都是個人資料，當中包括身份證明文件(例如香港身份證及職員/學生證)、姓名、地址、電話、病歷、受僱紀錄、錄音、錄影片段及相片等。

2. 香港中文大學(大學)是負責任的公營機構，在處理和使用個人資料時務須嚴守《個人資料(私隱)條例》所載的規定，確保儲存的個人資料準確無誤，及有妥善的儲存方法，並依照在收集資料時所說明的目的使用該等資料。所有教職員和同學處理可供辨認的個人資料時務須提高警惕，確切遵守有關個人資料(私隱)的法例，並採取有效的保安措施，確保個人及敏感資料受到保障，當中包括教職員、學生、校友、病人、服務對象、捐款者、職位申請人、以及研究、實驗及調查所涉及的資料當事人的資料。

3. 請詳細閱讀《個人資料(私隱)條例》及相關的實務守則和指引，尤其六項保障資料原則，都刊載於大學有關「保障個人資料(私隱)」的網頁：http://www.cuhk.edu.hk/policy/pdo/b5/。如要查詢《個人資料(私隱)條例》其他資料，請瀏覽香港個人資料私隱專員公署的網頁：http://www.pcpd.org.hk。

4. 副校長(行政)及大學秘書長吳樹培先生為大學的保障資料主任。

預防措施

5. 各學系系主任、學院院長及部門主管必須審慎檢討及改進其轄下處理個人及敏感資料的程序，以及其他有關的內部執行安排，務必依照資訊科技服務處及大學其他相關行政部門不時發布的指引辦理(例如人力資源處於二〇一八年十月發出與僱傭有關的個人資料通函)。有關指引已刊載於上述大學有關「保障個人資料(私隱)」的網頁。各學系、學院及部門務須以加密程序及設定安全密碼方式，保障可供辨認的個人及敏感資料。桌上型電腦、手提電腦及便攜式儲存裝置內所有載有可供辨認的個人及敏感資料的檔案須加密或使用安全密碼保護<https://www.itsc.cuhk.edu.hk/user-trainings/information-security-best-practices/guidelines-for-data-protection/use-encryption-to-protect-confidential-data>，或使用 Azure 資訊保護 (AIP)<https://www.itsc.cuhk.edu.hk/images/content/privacy-security/aip/AIP_User_Guide-v2.0.pdf>。各教職員及同學欲以電郵傳送載有可供辨認的個人及敏感資料的附件應確保該等資料已加密或使用安全密碼保護，亦應確保電郵只傳送至指定收件人(見<http://www.cuhk.edu.hk/policy/pdo/>的相關貼士及指引)。如有需要，可請資訊科技服務處提供意見及協助：http://servicedesk.itsc.cuhk.edu.hk。

各學系系主任、學院院長及部門主管亦須確保在其學系/學院/部門內設立有效機制，以決定是否有必要使用流動電子計算器材及可移除的儲存載體處理可供辨認的個人及敏感資料，並確保該等器材獲妥善保管，而儲存在內的資料應以安全密碼及加密程序保護，同時

亦建議大學成員採用屬於部門而非個人的流動/可移除的儲存載體儲存資料。請詳細閱讀 *Guidelines for Securely Managing Mobile and Removable Devices* <https://www.itsc.cuhk.edu.hk/user-trainings/information-security-best-practices/guidelines-for-securely-managing-mobile-removable-devices> 及「*使用便攜式儲存裝置指引*」<http://www.cuhk.edu.hk/policy/pdo/b5/doc/portable_storage_c.pdf>。

直接促銷

6. 各教職員及同學須閱讀《2012 年個人資料(私隱)(修訂) 條例》中與規管直接促銷活動有關的條文。條文要求資料使用者須事先通知，並取得當事人的同意，才可使用其個人資料或將資料轉交第三者以作直接促銷產品／服務之用，而資料當事人不回應不能被視為同意。大學的直接促銷活動不單指索求捐贈或貢獻，更指向學生、校友及其他持份者宣傳課程/學科/服務的活動。詳情請參閱《直接促銷新指引》<http://www.pcpd.org.hk/chinese/publications/files/GN_DM_c.pdf>。

歐洲聯盟《通用數據保障條例》

7. 歐洲聯盟的《通用數據保障條例》已於 2018 年 5 月 25 日生效，當中涉及新的規定和加強的權利。GDPR 取代了整個歐洲的現有資料保護法，並引入重大變化及額外要求，對世界各地的企業，無論他們在何處經營，均造成廣泛影響。詳情請參閱歐洲聯盟《通用數據保障條例》2016 <https://www.pcpd.org.hk/tc_chi/data_privacy_law/eu/files/eugdpr_c.pdf>。

涉及第三方服務供應商

8. 各學系、學院及部門如聘用學生助理、承辦商等提供第三方服務，而他們有機會接觸個人及敏感資料或只限內部傳閱的資料，就必須與相關人士簽署「不洩密協議」，以防止遺失或未經授權使用或披露個人及敏感資料。請參閱大學有關「保障個人資料(私隱)」的網頁所載詳細資料及協議的樣本。

資訊保安事件報告政策

9. 各教職員和同學如發現或懷疑有違反個人資料(私隱)法例的事件，例如遺失儲存有可供辨認的個人或敏感資料的裝置或文件，必須立即：
   (1) 填寫「資訊保安事件報告表格」；
   (2) 將該表格以機密電郵立即傳送資訊科技服務處處長(資訊科技事件)或秘書處(非資訊科技事件)；及
   (3) 盡快向有關的學系系主任、學院院長及部門主管報告事件，以便大學即時採取補救行動，防止或減低對資料當事人、大學或其他相關人士造成的傷害。請參閱大學有關「保障個人資料(私隱)」的網頁所載政策的詳情和有關表格。

恪守法例

10. 大學對資料當事人的私隱極為重視，竭力保障所收集及管理的個人資料，並恪守個人資料(私隱)的有關法例。這方面的工作有賴全體教職員和同學通力合作，校方謹此向各位表達衷心感謝！

副校長(行政) 及大學秘書長
吳樹培
二〇一八年十一月十五日