

法規名稱：臺北市立天文科學教育館個人資料保護管理要點

制(訂)定日期：民國 111 年 03 月 31 日

當次沿革：中華民國 111 年 3 月 31 日奉首長核定以電子郵件下達訂定全文 44 點

壹、總則

一、臺北市立天文科學教育館（以下簡稱本館）為落實個人資料蒐集、處理或利用法令、尊重當事人資訊自決權、促進個人資料合理利用及避免人格權受侵害，特依個人資料保護法（以下簡稱本法）、個人資料保護法施行細則（以下簡稱本法施行細則）及其他相關法令規定，訂定本館個人資料保護管理要點（以下簡稱本要點）。

二、本要點適用於本館及受本館委託或與本館共同蒐集、處理或利用個人資料其他公務機關或非公務機關。但其他法令另有規定者，從其規定。

貳、個人資料保護管理組織

三、為落實個人資料保護及管理，特設置本館個人資料保護管理執行小組（以下簡稱本小組）。

四、本小組任務如下：

- （一）本館個人資料保護政策擬議。
- （二）本館個人資料管理制度推展。
- （三）本館個人資料隱私風險評估及管理。

- (四) 本館各組室（以下簡稱各組室）人員個人資料保護意識提升及教育訓練計畫擬議。
- (五) 本館個人資料管理制度適法性與合宜性檢視、審議及評估。
- (六) 其他本館個人資料保護、管理規劃及執行事項。

五、本小組設召集人及執行秘書各一人，由本館首長指定人員兼任；其餘委員由各組室主管或其職務代理人擔任。

六、本小組會議視業務推動需要不定期召開，由召集人主持；召集人因故不能主持會議時，得指定成員代理。本小組開會時，得邀請相關業務組室人員或學者專家出（列）席。

七、各組室委員應指定專人辦理組室內下列事項：

- (一) 個人資料被竊取、洩漏、竄改或其他侵害事件（以下簡稱個資事件）。
- (二) 本法第十條及第十一條第一項至第四項所定請求事項之考核。
- (三) 本法第十一條第五項及第十二條所定通知事項之考核。
- (四) 本法第十七條所定公開或供公眾查閱。
- (五) 本法第十八條所定個人資料檔案安全維護。
- (六) 個人資料保護事項協調聯繫。
- (七) 組室內個人資料損害預防及危機處理應變通報。
- (八) 組室內個人資料專人名冊之製作及更新。
- (九) 組室內個人資料專人教育訓練名單及紀錄之彙整。

(十) 其他組室內個人資料保護管理規劃及執行。

八、執行秘書應協助本館個人資料保護法令諮詢。

參、個人資料蒐集、處理或利用內部管理程序

九、各組室蒐集、處理或利用個人資料，其類別、數量及接觸人員應符合本法第五條比例原則，以處理法定職務必要範圍內為限，儘量以蒐集最少且不含本法第六條所定個人資料為原則。

各組室蒐集、處理或利用個人資料特定目的，以本館已依適當方式公開者為限；有變更者，亦同。

十、各組室蒐集當事人個人資料時，應明確告知當事人本法第八條第一項所列事項。但符合本法第八條第二項規定情形之一者，不在此限。

各組室蒐集非由當事人提供個人資料時，應於處理或利用前，向當事人告知個人資料來源及本法第八條第一項第一款至第五款所列事項。

但符合本法第九條第二項第一款至第四款規定情形之一者，不在此限。

依前二項規定告知當事人，其告知事項內容應使用通俗、簡淺易懂語文，避免使用艱深費解詞彙。

依第一項及第二項規定告知當事人，如有委託或共同蒐集、處理或利用個人資料，應同時告知委託或共同利用情形。

依第一項及第二項規定告知當事人，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件、明顯或適當處所公告或其他足以使當事

人知悉或可得知悉方式為之。

十一、各組室依本法第六條第一項第六款、第十一條第二項但書或第三項但書規定，經當事人書面同意者，應取得當事人同意書面文件；該書面文件作成方式，依電子簽章法規定，得以電子文件為之。

各組室依本法第十五條第二款或第十六條但書第七款規定經當事人同意者，應符合本法第七條及本法施行細則第十五條所定方式。

十二、各組室蒐集或處理個人資料應符合下列情形之一，並於蒐集時註明蒐集特定目的項目及代號：

- (一) 依本館組織規程或本法第十五條第一款及本法施行細則第十條所稱執行法定職務。
- (二) 經當事人同意。
- (三) 依法受委託執行職務。

十三、對滿七歲未成年人蒐集或處理其個人資料，有下列情形之一者，得經未成年人本人同意為之，其他情形應得其法定代理人同意：

- (一) 依其年齡及身分、日常生活所必需。
- (二) 純獲法律上利益（純粹取得權利或不負任何義務）。
- (三) 法定代理人事前允許處分財產或營業。

對未滿七歲未成年人及受監護或輔助宣告人蒐集其個人資料，應得其法定代理人同意。

法定代理人基於保護未成年人及受監護或輔助宣告人利益，得行使

本法第十條或第十一條第一項至第四項規定權利。

本點關於未成年人保障未盡事宜，依民法及兒童及少年福利與權益保障法等相關規定辦理。

十四、各組室應優先考慮以去識別化或經遮蔽個人資料為處理或利用。

十五、任何非原蒐集特定目的外利用，各組室應確認符合本法第十六條但書規定後始得為之，並將利用歷程作成紀錄。

前項情形，宜審酌個案狀況，規劃當事人選擇不同意或退出同意機制。

十六、個人資料檔案屬檔案法所稱檔案者，其申請閱覽、抄錄或複製，應依檔案法、檔案法施行細則及臺北市政府檔案應用相關規定辦理。依政府資訊公開法申請公開或提供前項規定以外政府資訊，如涉及個人資料特定目的外利用，應審酌是否具有本法第十六條但書及政府資訊公開法第十八條第一項第六款所定情形。

十七、各組室對於個人資料利用，不得為資料庫恣意連結，且不得濫用。

十八、本館保有個人資料有誤或缺漏時，應由資料蒐集組室簽奉核定後，移由資料保有組室更正或補充之。

因可歸責於本館事由，未為更正或補充個人資料，應於更正或補充後，由資料蒐集組室以通知書通知曾提供利用對象。

十九、本館保有個人資料正確性有爭議者，應由資料蒐集組室簽奉核定後，移由資料保有組室，視個人資料載體性質為適當停止處理或利用該個人資料，並註明原因。但符合本法第十一條第二項但書情形者，不在此限。

二十、各組室應定期查明蒐集或處理個人資料適用法令所訂定保存期間；未明定者，視執行業務必要性及合理性，於本館年度檔案分類及保存年限表明定，或訂定告知當事人合理保存期間。

本館保有個人資料蒐集特定目的消失或期限屆滿時，應由資料蒐集組室簽奉核定後，移由資料保有組室，視個人資料載體性質為適當停止處理或利用。但符合本法第十一條第三項但書情形者，不在此限。

二十一、各組室依本法第十一條第四項規定停止蒐集、處理或利用個人資料者，應簽奉核定後移由資料保有組室，視個人資料載體性質適當為之。

二十二、個人資料有補充、更正、停止處理或利用、刪除時，應通知曾利用其他機關或組室；或與其他機關或組室事先協調及規劃個人資料

料定期更新機制。個人資料依規定刪除或停止處理、利用前，應對相關系統或服務作影響評估並妥為因應。

二十三、個人資料刪除，應檢查是否達到資料無法還原或再組合程度，並得參考機關檔案保存年限及銷毀辦法及臺北市政府公務機密維護作業等相關規定辦理。

二十四、各組室將個人資料作國際傳輸前，應確認法令限制及他國（境）對個人資料保護法令要求，並做適當保護措施。

肆、機關間個人資料交換運用內部管理程序

二十五、本館與臺北市政府其他所屬機關（以下簡稱本府其他機關）交換運用個人資料，依本要點規定辦理；本要點未規定者，適用本要點其他規定。

二十六、本要點所稱交換運用，指本館為與本府其他機關共同執行法定職務，或協助本府其他機關執行法定職務，而以臺北市政府（以下簡稱本府）名義蒐集個人資料，並將所蒐集個人資料提供予各該本府其他機關。

二十七、本館為辦理交換運用，應於蒐集個人資料前，確認所涉本府其他

機關法定職務依據、特定目的、需提供個人資料類別、利用期間、地區、對象及方式，經簽會臺北市政府法務局並簽報本府同意後，始得為之。

前項所定應確認事項，應於蒐集個人資料前，以機關名義明確告知當事人。但有第十點第一項但書或第二項但書所定情形者，不在此限。

依前二項規定辦理交換運用，視為本法第二條第四款及本法施行細則第六條第二項所定內部傳送。

伍、當事人權利行使

二十八、當事人依本法第三條、第十條或第十一條第一項至第四項規定向本館請求答覆查詢、提供閱覽、製給複製本、更正、補充、停止蒐集、處理、利用或刪除個人資料時，應經身分確認程序，並得視情形請當事人檢附相關證明文件或做適當釋明。

第一項證明文件內容如有遺漏、欠缺或釋明不完整，應通知限期補正。

申請案件有下列情形之一者，應以書面或電子文件駁回其申請：

- (一) 申請文件內容有遺漏、欠缺、虛偽不實或釋明不完整，經通知限期補正，逾期仍未補正或無法補正。
- (二) 有本法第十條但書各款情形之一。
- (三) 有本法第十一條第二項但書或第三項但書所定情形之一。
- (四) 與法令規定不符。

第一項請求處理期限及延長，依本法第十三條規定辦理。

二十九、當事人請求閱覽、抄錄或複製個人資料，得依檔案閱覽抄錄複製收費標準收取費用。

前項情形，由承辦組室派員陪同為之。

三十、各組室提供當事人閱覽、抄錄或複製個人資料前，應確認未同時揭露他人個人資料。

三十一、本館保有個人資料檔案以公開於本館網站個人資料保護專區為原則，並應於建立個人資料檔案後一個月內為之；更新檔案時，亦同。

為確保當事人有充分表達意見機會及申訴管道，本館網站個人資料保護專區，應設有個人資料客訴聯絡方式。

陸、委外監督

三十二、各組室研擬業務委外招標文件時，應就委外範圍擬定投標廠商須具備個人資料保護管理能力，於招標文件訂定評選項目或於採購契約訂定監督事項及罰則條款，並將本要點列入採購契約文件供廠商遵循。

三十三、契約終止、解除或屆滿時，廠商應返還或刪除所保有個人資料，或交接本館指定其他組室，刪除存取權限，並切結未以任何形式保留備份或影本；續約廠商不在此限。

履約期間廠商員工離職或留職停薪，應說明所負責系統存取權限及完成鎖定帳號或停止系統權限，並應更換離職或留職停薪員工曾接觸密碼。

三十四、各組室於履約期間應定期確認廠商執行個人資料保護措施並予以記錄，前項措施如保密切結書及同意書等。

前項保護措施如保密切結書及同意書等皆屬之。

柒、個人資料風險評估及安全維護

三十五、各組室電子處理個人資料安全維護，應遵守資通安全管理法、資通安全管理法施行細則、檔案法、檔案法施行細則、臺北市政府及所屬各機關辦理資訊使用管理稽核作業規定、臺北市政府文書處理實施要點及臺北市政府資通安全等相關法令規定（以上皆以最新版為主），並得參考行政院國家資通安全會報技術服務中心所訂各項資訊安全參考指引辦理。

非電子處理個人資料安全維護，應依檔案法、檔案法施行細則、臺北市政府文書處理實施要點、臺北市政府公務機密維護作業等規定辦理。

本館得因應最新技術發展或資訊安全問題訂定技術指引。

各組室得因應負責業務特性自訂內部安全控制措施或管理細則。

三十六、定期執行個人資料盤點作業，作業項目依序如下：

（一）清查各作業流程中所使用表單、紀錄，並辨識其中與個人

資料有關者，歸納整理成個人資料檔案。

- (二) 使用個人資料盤點表或其他具相同效用技術、軟體或表單，檢視其保有個人資料檔案，確認個人資料檔案名稱、保有依據及特定目的、個人資料種類。
- (三) 使用個人資料盤點表或其他具相同效用技術、軟體或表單，檢視其保有個人資料檔案生命週期，包含蒐集、處理、利用內容。
- (四) 依第一款至前款檢視結果，建立個人資料檔案清冊。

前項個人資料盤點表及個人資料檔案清冊，包括以下個人資料相關欄位：

- (一) 所涉主要業務、職掌內容及办理流程。
- (二) 個人資料檔案名稱。
- (三) 業務主管組室。
- (四) 保存管理組室。
- (五) 保管方式。
- (六) 檔案型態，包括紙本類、電子類、可攜式媒體內電子檔及系統資料庫。
- (七) 個人資料來源。
- (八) 法令或契約上保有依據。
- (九) 是否須履行本法所定告知義務。
- (十) 特定目的（依本法特定目的及個人資料類別填寫）。
- (十一) 個人資料類別（依本法特定目的及個人資料類別填寫）。
- 。
- (十二) 個人資料項目。
- (十三) 本法第六條所定個人資料項目。
- (十四) 個人資料數量。

- (十五) 內部進行蒐集、處理或利用組室。
- (十六) 外部進行蒐集、處理或利用者。
- (十七) 委外及受委託對象接觸情形。
- (十八) 法定或自訂保存期限。
- (十九) 銷毀方式。
- (二十) 是否依本法第十七條規定對外公告。
- (二十一) 備註。

三十七、本館應依前點所定盤點作業結果，規劃並定期執行個人資料風險評估作業，其評估必要項目如下：

- (一) 個人資料可識別程度。
- (二) 個人資料檔案型態及數量。
- (三) 個人資料類別敏感性及風險性。
- (四) 蒐集、處理、利用過程及環境。
- (五) 個人資料存取頻率及存放位置。
- (六) 蒐集、處理、利用及保有適法性。
- (七) 個人資料保護意識及相關知能。

本館應依前項所定風險評估結果，規劃並採取必要風險控管及精進措施。

三十八、各組室應視業務性質保存下列紀錄或證據：

- (一) 當事人書面同意。
- (二) 告知或通知當事人。
- (三) 當事人或法定代理人依本法第十條或第十一條第一項至第

四項定主張權利。

(四) 蒐集、處理、利用個人資料所生軌跡紀錄。

(五) 本館或各組室檢查或稽核。

(六) 個人資料正確性有爭議。

(七) 個資事件。

依前項規定保存紀錄或證據，除其他法令另有規定或契約另有約定外，應至少保存五年。

三十九、為妥善因應個資事件，各組室平時應建立通報及支援聯絡網人員名冊，掌握個人資料處理或利用流程，透過監測資料注意異常狀況潛在問題。

四十、負責蒐集、處理或利用個人資料職員工，應定期參加個人資料保護教育訓練。

新進職員工或參與本館招標第一次得標廠商員工，應詳閱本要點、相關契約內容，得標廠商宜視需求提供必要之教育訓練。

專人應適時通知個人資料保護注意事項，並應視需要轉知業務往來之其他機關或組室。

四十一、個資事件發生時，各組室應依指示及視事件性質，於三十六小時內採取下列應變措施：

(一) 中斷入侵或洩漏途徑。

(二) 緊急儲存尚未被破壞資料。

- (三) 啟動備援程序或替代方案。
- (四) 事件原因初步分析。
- (五) 評估受侵害個人資料類別及數量。
- (六) 檢視防護及監測設施功能。
- (七) 記錄事件經過。
- (八) 行政內部調查完成前保存相關證據。
- (九) 解決或修復方案。
- (十) 通知保有相同資料組室。
- (十一) 洽商專業人員協助或進駐處理。
- (十二) 涉及刑事責任者，移請檢警鑑識或調查。
- (十三) 發布新聞稿、網站公告或其他可告知當事人方式。

四十二、個資事件發生後，本館應依本法第十二條通知當事人，內容包括侵害事實及因應措施說明、建議當事人處理事項、提供查詢及協助管道、賠（補）償當事人處理事務相關費用等補救措施。

前項通知，指以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉方式為之。

四十三、個資事件發生後，各組室應於知悉後一小時內完成通報作業。通報對象為資安小組，並副知召集人及執行秘書；通報內容至少應包括通報人身分、資料外洩或侵害方式、時間、地點、初估外洩或侵害個人資料類別及數量、避免損害擴大處置等資訊；通報方式以電話或簡訊為主，電子郵件為輔。

捌、附則

四十四、本館為因應法令修訂、技術發展或強化人格權保障，應為必要補充及調整，並適時修正本要點。