# (機關名)

# 應用教育部國民及學前教育署

# ○○○○資料管理規定範本

申請機關 (以下簡稱機關)為應用教育部國民及學前教育署資料，特訂定本規定。

1. 依據

【以下為範例，請依實務調整】

本機關使用教育部國民及學前教育署(以下簡稱國教署)資料，應遵守個人資料保護法（以下簡稱個資法）第五條、第六條、第十五條、第十六條、第十九條及第二十條規定辦理。取得資料之法源依據如下：

(請機關詳列使用國教署資料之所有法源依據)

二、 目的

【以下為範例，請依實務調整】

1. ○○○○○○○○ (以下簡稱「○○機關」)，因辦理○○○○○○○業務需要，必須使用○○○○○○○○○資料(以下簡稱本資料)，以達○○○○○○○○○目的。為落實資通安全及個人資料之保護管理，防止資料不當使用或外洩，保障個人隱私，遵循「個人資料保護法」之規定，茲訂定「(機關名)應用教育部國民及學前教育署○○○○資料管理規定」(以下簡稱「本規定」)。
2. 本規定之目的，在兼顧個人隱私權的保護及個人資料的合理利用，建立機關對個人資料蒐集、處理及利用之程序，落實對個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏，並尊重當事人對權利之行使及諮詢。
3. 為發揮資訊資源共享效益，提高行政效能，確保資通安全暨個人資料保護，特訂定本規定。

三、 機關業務應用範圍 (含持有機關、使用機關、委外受託單位及其複委託單位)

【以下為範例，請依實務調整】

|  |  |  |
| --- | --- | --- |
|  | 持有、使用機關  名稱 | 實際運用狀況  (例如：資料維護、資料分析或資料管理……等事項) |
| 持有機關 |  |  |
| 使用機關 |  |  |

(請機關詳述使用國教署資料之所有單位)

四、 督考查核及相關稽核措施

○○○○○○○○(機關名稱)及業務應用範圍(持有、使用機關)使用本資料，應依業務別向國教署申請經同意後使用，並依本規定管理、查核及接受稽核。

五、 個人資料之範圍

【申請機關應敘明所需之資料內容、範圍，以及其與取得資料法律依據之合理必要關聯性，並以取得最小化個人資料即能達成目的為原則，禁止過度蒐集個人資料。】

1. 特定目的項目： 等運用。

【製作指引：本項請依「個人資料保護法之特定目的及個人資料之類別」，說明特定目的項目，例如：人事管理(○○二)、全民健康保險、勞工保險、國民年金保險或其他社會保險(○三一)、消費者、客戶管理與服務(○九○)等。】

1. 個人資料定義：

參照個人資料保護法第二條第一款。

(請機關詳述使用個人資料之特定目的項目，若向國教署要求提供連結作業之資料不含個人資料，本段落可刪除)

六、 個人資料之蒐集、處理與利用方式

1. 機關(並含持有機關、使用機關)依前條個人資料蒐集之特定目的及必要性，蒐集、處理及利用個人資料，並定期清查所保有之個人資料現況。
2. 機關所屬人員為執行業務所蒐集或委託他人蒐集之個人資料，均視為機關所蒐集持有，並接受監督。
3. 機關委託其他人、持有機關、使用機關蒐集、處理或利用個人資料之全部或一部時，機關應對受託者為適當之監督並與其明確約定相關監督事項。
4. 機關指定之專責人員定期清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之個人資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。資料刪除程序依機關內部規定流程辦理。
5. 機關(並含持有機關、使用機關)所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合個人資料保護法之規定。

(若向國教署要求提供連結作業之資料不含個人資料，本段落可刪除)

七、 個人資料之處理和利用是否會進行國際傳輸? □是 □否； 法源依據條列如下：

(請機關詳述處理和利用國教署資料進行國際傳輸之所有法律依據)

八、 事故之預防、通報及應變機制

【以下為範例，請依實務調整】

本機關將遵循個資法第十八條和第二十七條規定，由專人辦理安全維護事項，採行適當之安全措施，妥善使用國教署資料。資料連結介接機關(申請機關或持有、使用機關)如發生個人資料安全事故，或疑似事故時，應依相關法令採取必要之緊急應變措施，查明事故原因、責任釐清及避免損害擴大之防免措施，且應即時通報本署並提供前開相關資料。對於個人資料遭竊取、竄改、毀損、滅失、洩漏等個資事故之當事人，申請機關應依個人資料保護法第12條之規定，以書面或電子化形式通知當事人說明，使其知悉並說明機關已採取之處理措施。另應針對事故發生原因研議改進措施。

九、 資料安全管理、資料使用者管理及設備安全管理

【以下為範例，請依實務調整】

1. 資料安全管理：
2. 需指定專責人員辦理安全維護事項：
   1. 應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
   2. 應敘明專責人員就系統連結介接資料應辦理之安全維護事項，並造冊列管所有使用、查詢資料人員之相關管理措施。
   3. 專責人員應依資通安全管理法、資通安全責任等級分級辦法及其資通安全責任等級之公務機關應辦事項，接受並完成相應之資通安全教育訓練。
3. 電腦存取個人資料之管控：
   1. 應妥善保管個人電腦存取資料之硬體，並設定登入及螢幕保護程式密碼。個人資料使用完畢，應即退出電腦使用檔案，不得留置於電腦上。下班前應關閉電腦電源，並將所保有其他個人資料之媒介物置於專用抽屜內上鎖保管。
   2. 機關(並含持有、使用機關)同仁如因其工作職掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。
   3. 個人資料檔案使用完畢應即退出，不得任其停留於電腦畫面上。
   4. 定期進行電腦系統防毒、掃毒之必要措施。
   5. 特種個人資料（如病歷、醫療、基因、性生活、健康檢查、犯罪前科）應另加設管控密碼始得存取。
   6. 置放個人資料電子檔案之個人電腦，不得直接作為公眾查詢之前端工具。
4. 紙本資料之保管：
   1. 機關(並含持有、使用機關)保有個人資料存在於紙本者，應儲存於上鎖之保管箱或檔案室內，僅業務主管有開啟調閱權限，其他所屬人員因業務需要而須調閱或使用個人資料者，應提出申請，經業務主管人員同意後調閱或使用。非經機關首長批核同意不得任意複製或影印。
   2. 儲存個人資料紙本之保管箱或檔案室內，應設置防火裝置及防竊措施。
   3. 個人資料之紙本丟棄時，應先以碎紙設備進行銷毀處理。若屬大批量個人資料紙本，可採水銷方式銷毀。
5. 資料使用者管理：

【以下為範例，請依實務調整】

1. 使用者申請程序及管理
   1. 帳號新增或異動須經申請，申請時應列明本資料查詢權限，並由權責主管核可後，交由管理者配賦帳號及查詢權限，且保留紙本申請單（如屬線上申請簽核則免）及電腦紀錄。
   2. 本資料應用含所屬機關(單位)，採分層負責。資訊單位設系統及機關管理者，業務單位設系統群組管理者，群組管理者經核准後由機關管理者建置，使用者經單位核准後向所屬業務單位提出申請，由業務單位系統群組管理者建置。各單位管理者及使用者均應提出申請，並經機關或單位核准後由權責管理者建置。
   3. 帳號及密碼通知過程應具保密措施，防止被竊視及竊取。
   4. 管理者及使用者不得使用非本人申請之帳號，帳號不得交接予他人，且不得和他人共用。
   5. 密碼長度應至少12 個字元以上，必須包含至少一個大寫、一個小寫英文字母、符號及數字(4 擇 3)組成，系統每 3 個月要求使用者定期更改密碼，使用者密碼應妥善保管，避免他人知悉。
   6. 系統限制使用者連續登入密碼失敗 3 次即鎖碼，並經申請核准後，由管理人員解除帳號鎖碼。
   7. 使用者職務異動時，應於職務異動前辦理帳號異動程序，並於異動前或當日，由管理人員停止原帳號。
   8. 管理者職務異動時，應於職務異動前辦理帳號異動程序，並於異動前或當日，由承接之新任管理者於承接業務時停止原管理者帳號，並新增新管理者帳號，機關之系統無法變更管理者帳號時，新任管理者應立即變更管理者密碼。
2. 管理者應每半年辦理帳號清查，檢視使用者權限，並廢止重複、閒置、職務調整、離職及退休者帳號。
3. 機關(並含持有、使用機關)申請○○○○○○○○(資通系統名稱)資料連結作業單位主管及承辦人異動時，應函知國教署。
4. 設備安全管理：
5. 建置個人資料之有關電腦設備，應定期修補作業系統安全性更新，維持軟體和應用程式為最新版本，以避免有安全性漏洞遭駭客入侵竊取個資。
6. 儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。主機置放之機房應設置門禁、監視錄影及消防滅火設備。
7. 處理或保有個人資料之個人電腦，必須啟動 OO 分鐘(例如:10 分鐘)以內具密碼設定之螢幕保護機制，且不得直接作為公眾查詢之前端工具。
8. 應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。
9. 機關保有之個人資料檔案應定期(例如：每二週)備份；當更新設備時，應注意備份資料或備份載體之安全保護措施。
10. 重要個人資料備份應異地存放，並應建置防止個人資料遭竊取、竄改、毀損、滅失或洩漏等事故之機制。
11. 電腦、行動裝置或其他可攜式儲存媒體需報廢汰換或轉作其他用途時，機關主管應檢視該設備所儲存之個人資料是否確實刪除。
12. 更新或維修電腦設備時，應指定專人在場，確保個人資料之安全及防止個人資料外洩。
13. 電腦設備報廢或不使用時，確實刪除電腦硬體設備中所儲存之個人資料檔案。

十、 資料安全管制作業

【以下為範例，請依實務調整】

1. 查詢資料之管制措施
2. 申請機關、持有機關、使用機關查詢國教署資料時，應填寫或輸入案號及查詢事由，作為日後查核依據。
3. 查詢國教署資料應避免非業務權責人員閱覽、擷取及破壞。
4. 查詢國教署資料完竣後，如有併案或附卷必要，應妥善保管，紙本應依公文檔案管理辦法管理保存，電子檔應有存取權限控管。
5. 連線查詢國教署資料逾時，系統應自動登出。
6. 系統應記錄查詢者帳號、查詢日期、時間、查詢作業代號、被查詢者查詢條件、查詢案號及查詢事由等查詢日誌，並保留 5 年。
7. 批次取得國教署資料或異動資料管制措施
8. 檔案傳輸或磁性媒體交換方式批次取得國教署資料及異動資料者，應由專人辦理，並檢核資料完整性。
9. 取得資料載入系統應用時，應設定使用該資料之存取權限及核准使用期限。欲使用資料者，須經申請核准後始得使用，並應於核准期限內使用及應用於核准業務範圍。
10. 資料檔案儲存於可攜式儲存媒體者，應置放於安全場所，應上鎖或管制人員進出。
11. 國教署資料不得任意複製，如有複製資料之業務需要，應經申請核准後，始得複製，資料傳送時應採取適當的保密措施。
12. 資料銷毀程序
13. 線上查詢或經由網路取得國教署資料檔，應指定專人或由系統定期清除，以防範資料被不當存取。
14. 線上查詢國教署資料完竣後，如可銷毀，紙本文件應銷毀至無法辨識，電子檔如無保留必要性，應即刪除。
15. 儲存於電腦設備或系統之資料檔案，使用完竣且確認無保存必要，應簽報單位主管核定後，刪除資料檔案，並確認其資料檔案無法復原。
16. 儲存於可攜式媒體之資料檔案，使用完竣且確認無保存必要，應簽報單位主管核定後，辦理銷磁或銷毀作業。
17. 機關每年應檢視已申請核准之國教署資料連結作業之使用情形，如已無需求者，應函請國教署終止該連結作業。

十一、 資料安全定期稽核機制

【以下為範例，請依實務調整】

1. 機關所屬業務單位每月列印查詢紀錄單，供查核人員查核，每月抽 查比率至少為百分之○，每月抽查筆數不得少於 10 筆，查詢總筆數少於 10 筆者，應全數查核。
2. 前項查核結果，應至少保留5年備查，經發現有異常狀況者，機關所屬業務單位會同政風單位及資訊單位共同調查，並要求限期提出說明或進行改善，調查結果另作成稽核紀錄備查。
3. 機關應至少每年辦理1次機關及持有、使用機關稽核工作，查察是否落實本規定事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行，所有稽核工作均應作成稽核紀錄，保留5 年備查。
4. 國教署實施稽核作業時，本機關須配合提供相關查核資料、持有機關、使用機關、使用單位及使用者，且須配合辦理。
5. 國教署如發現資料連結介接機關(含申請、持有、使用機關)及其所屬機關有妨礙、規避、變更相關管理功能或技術，或違反本規定者，得通知其限期改善，屆期未改善者，暫停其資料連結介接作業。
6. 經依前款規定暫停資料連結介接作業者，申請機關如，應於完成改善事項後，向國教署提出申請，經同意後始可回復連結作業；連結作業暫停逾6個月始完成應改善事項者，如欲回復連結作業，應重新提出申請。

十二、 個人資料安全維護之整體持續改善

【以下為範例，請依實務調整】

1. 隨時依據執行狀況、相關技術發展及法令修正等事項，檢討本管理規定是否合宜，並予必要之修正。
2. 針對個資或資安稽核結果，有不符合法令之虞者，應規劃改善與預防措施。

十三、 業務終止後個人資料處理方法

【以下為範例，請依實務調整】

申請機關如欲終止連結作業，應於終止日一個月前以書面通知國教署。

十四、 法律責任

【以下為範例，請依實務調整】

自國教署取得之資料須負保密責任，未經國教署同意，不得作任何未經授權之蒐集、處理及利用，並以其他方式告知、交付、移轉予第三方；如有不當使用或侵害個人隱私，除應依相關規定追究行政責任外，若違反刑法、個人資料保護法或其他相關法令者等，將依法辦理。

特此聲明

機關名稱：

機關首長：＿＿＿＿＿＿＿＿＿＿＿＿＿＿

簽署日期：＿＿＿＿＿＿＿＿＿＿＿＿＿＿

**中華民國 年 月 日**