明愛胡振中書院

Caritas Wu Cheng-chung College

保護個人資料政策

2024 年 9 月

◆ 目的：本校為貫徹執行「個人資料（私隱）條例」的原則及規定，使個人資料得到適當的保護及處理。

甲、使個人資料得到適當的保護及處理的相關政策：

1. 所有學生個人資料檔案收存於上鎖鋼櫃內，置放於校務處。鋼櫃保持上鎖，由校長及有關管理人員掌管鋼櫃鎖匙。

2. 學生輔導個案紀錄、學生訓育資料收存於上鎖鋼櫃內，置放於訓輔主任室。鋼櫃保持上鎖，由副校長、訓、輔主任掌管鋼櫃鎖匙。

3. 學生點名冊只顯示學生姓名及性別。

4. 「家長簽名及緊急聯絡電話」只由校長及班主任妥善保管，以便日常聯絡家長。

5. 所有關於學生或家長的個人資料（例如學生行為紀錄、病歷等），未經家長同意，不得公開。

6. 在需要收集個人資料的時候（不論是學生通告或網頁表格），須參考保護個人資料原則，詳列「收集資料的目的及方式」、「個人資料的準確性及保留期間為基於人資料被使用於或目的所需時間」、「個人資料的保安」、「個人資料所作的主要用途」以及「查閱及改正其個人資料」等重要原則。

7. 每學年初全校發出通告，徵求家長授權學校可以將其子女的習作、活動相片等刊登於校訊、橫額、網頁等物品。

8. 為全校教師在教師休息室提供可以上鎖的櫃格，教師有責任將涉及學生或家長個人資料的文件鎖好，以免遺失。如有遺失，由該名教師承擔責任。

9. 每學年初向全體教師講解本校「保護個人資料政策及教職員理個人資料指引」；透過教師培訓，安排講座或工作坊，讓教師了解保障個人私隱的重要及相關條例的精神和執行情況。

10. 學校電腦行政管理系統（WebSAMS）只加密開放給本校教職員，教職員須以個人密碼登入使用，用後須按既定程序登出。

11. 本校備有「查閱/改正資料要求冊」供有關人士翻查或改正資料用。

乙、教師、書記及職工處理個人資料指引：

各教師、書記及職工必須詳閱下列指引及在處理有關資料時採用相應步驟， 確保個人資料得到適當的保護：

1. 處理載有學生或家長個人資料的文件（例如資助資格証明書）時，班主任應將未收齊的文件存放於教師休息室可上鎖櫃格內，並且鎖好，待全班文件收齊後交予負責主任或教師妥善存放。負責主任或教師必須將該等文件存放於可上鎖的文件櫃或抽屜內，並且鎖好。

2. 每學年初班主任獲校方分發之學生資料（例如家長簽名及緊聯絡電話等），必須鎖好，以免遺失或資料外洩，並於學年結束時按照校方的指示交回校務處。

3. 如有必要列印學校電腦行政管理系統（WebSAMS）之學生個人資料，教師有責任妥善保管該等資料，確保資料不會遺失或外洩。

4. 教師若有需要，可向校務處借用學生個人資料檔案。未經校方許可，教師不可複印檔案資料。使用完畢後盡快將檔案歸還校務處。

5. 在傳送載有個人資料文件的時候，須親自交予負責主任或教師，由負責主任或教師當面點收。

6. 任何情況下，不可將載有個人資料的文件放於資料使用者以外人士可以接觸的地方。

7. 教師每天離校前有責任檢視辦公桌及附近地面，以避免沒有將載有個人資料的文件遺留在資料使用者以外人士可接觸的地方。

明愛胡振中書院

Caritas Wu Cheng-chung College

Personal Data Protection Policy

September 2024

- Purpose: This school aims to implement the principles and regulations of the "Personal Data (Privacy) Ordinance" to ensure that personal data is appropriately protected and handled.

A. Policies related to the appropriate protection and handling of personal data:

1 All student personal data files are stored in a locked cabinet located in the school office. The cabinet remains locked, with the principal and relevant administrative personnel holding the keys.

2 Records of student counseling cases and student training data are kept in a locked cabinet in the counseling director's office. The cabinet remains locked, with the vice principal and the counseling director holding the keys.

3 The student attendance register only displays the student's name and gender.

4 "Parental signatures and emergency contact numbers" are kept securely by the principal and class teachers for the purpose of contacting parents.

5 All personal data concerning students or parents (e.g., student behavior records, medical histories) shall not be disclosed without parental consent.

6 When collecting personal data (whether through student notices or web forms), the principles of personal data protection must be referenced, detailing "the purpose and method of data collection," "the accuracy of personal data and retention period based on the time needed for its intended use," "the security of personal data," "the primary purposes for which personal data is used," and "the rights to access and correct personal data," among other important principles.

7 At the beginning of each school year, a notice is sent to all parents requesting authorization for the school to publish their children's work, activity photos, etc., in school newsletters, banners, websites, and other materials.

8 The school provides lockable cabinets in the teachers' lounge for all teachers. Teachers are responsible for securely locking any documents containing student or parent personal data to prevent loss. If lost, the teacher will bear responsibility.

9 At the beginning of each school year, all teachers are briefed on the school's "Privacy Policy and Guidelines for Staff on Personal Data." Through teacher training, lectures, or workshops are arranged to help teachers understand the importance of personal privacy protection and the spirit and implementation of relevant regulations.

10 The school's administrative management system (WebSAMS) is encrypted and accessible only to school staff. Staff must log in with personal passwords and must log out according to established procedures after use.

11 The school provides a "Data Access/Correction Request Form" for relevant individuals to review or correct their data.

B. Guidelines for Teachers and Office Staff Handling Personal Data:

All teachers and office staff must carefully read the following guidelines and follow the corresponding steps when handling related data to ensure that personal information is adequately protected:

1 When handling documents containing personal data of students or parents (e.g., eligibility certificates), class teachers should store any incomplete documents in a lockable cabinet in the teachers' lounge and secure them. Once all documents for the class are collected, they should be handed over to the responsible supervisor or teacher for proper storage. The responsible supervisor or teacher must keep these documents in a lockable cabinet or drawer and ensure they are locked.

2 At the beginning of each school year, class teachers receive student information (e.g., parental signatures and emergency contact numbers) from the school, which must be securely locked to prevent loss or data leakage, and returned to the school office at the end of the year according to the school's instructions.

3 If it is necessary to print student personal information from the school's administrative management system (WebSAMS), teachers are responsible for safeguarding this information to ensure it is not lost or leaked.

4 Teachers may borrow student personal data files from the school office if needed. Teachers are not allowed to make copies of the files without the school's permission. Files should be returned to the school office as soon as they are no longer needed.

5 When transmitting documents containing personal data, they must be delivered personally to the responsible supervisor or teacher, who should acknowledge receipt in person.

6 Under no circumstances should documents containing personal data be left in areas accessible to individuals other than the data users.

7 Teachers are responsible for checking their desks and surrounding areas before leaving school each day to avoid leaving documents containing personal data in places accessible to individuals other than the data users.