

TWGHs. S. C. Gaw Memorial College
Personal Data (Privacy) School Guidelines – General to Staff and Teachers

A. Purpose and manner of collection of personal data

1. Staff and teachers will ensure that the means of collection are fair and lawful. The means may include collecting forms in print format in person or by mail and in electronic format by fax or by e-mail, conducting face to face or telephone interviews with the Data Subject concerned.
2. School Administration Department will ensure that each of the purposes of collection is directly related to the functions or activities of the school and that the data collected in relation to a specified purpose is adequate but not excessive.
3. School Administration Department will inform the Data Subject explicitly of the following by way of verbal or written communication during collection of data:
 - i) the purpose(s) for which the data are collected;
 - ii) the group(s) of people to whom the data may be transferred;

B. Accuracy and duration of retention of personal data

1. All staff and teachers will ensure that data are not kept longer than necessary for the fulfillment of the purpose for which they are collected.
2. School Administration Department will alert the staff and teachers to whom the data are transferred, if any, of the return or disposal of the data at a specified date where appropriate.

C. Use of personal data

1. All staff and teachers should ensure that the personal data collected will not be used for any purpose(s) other than those for which the data was originally collected or a directly-related purpose without the prescribed consent of a Data Subject. School Administration Department should remind the staff and teachers to strictly adhere to this when transferring such data to them.

D. Security of personal data

All staff and teachers will protect the personal data collected/received from unauthorized access, processing, erasure or other uses by implementing the following arrangements:

1. *Staff and teachers access*

- i) Security measures must be adopted to ensure access to the data by authorized staff only, e.g., only the general office can access the data list of the students with xxxxxx
- ii) Measures must be in place to ensure the integrity, prudence and competence of such authorized persons, e.g., requiring them to participate in relevant training programmes/workshops.
- iii) Security precautions should be established to avoid staff taking any personal/sensitive data away from the working office.

2. *Data storage*

- i) An appropriate physical location should be identified where the personal data can be safely stored, e.g., in lockable filing cabinets or in rooms which can be locked when unoccupied, and files containing personal data should not be left open on desks or in areas where they can be seen by passers-by.
- ii) Measures should be adopted to ensure proper download of personal/sensitive data by authorized staff, especially through the Internet.
- iii) Personal/sensitive data should not be stored in portable devices, such as USB; in case personal/sensitive data have to be stored in portable device, permission must be granted from the School Administration Department while security measures must be imposed, such as data being encrypted or password-protected, to prevent data leakage due to accidental loss of the device or by leaving the device unattended.

3. *Data transmission*

- i) All staff and teachers should adopt appropriate measures to ensure the secure transmission of personal data, e.g., data being put in a sealed envelope marked 'confidential' with the addressee specified, data being encrypted or password-protected and the data recipients being double-checked to ensure that they are the right data transferees during electronic transmission.

4. *Data disposal*

- i) After the specified retention period, the disposal of personal data should be undertaken with appropriate security precautions to avoid any inadvertent disclosure to, or access by, unauthorized parties. For example, documents containing data held on paper should be shredded and a CD-ROM disk and a USB memory stick should be reformatted before disposal to avoid recovery of the data.

E. Reporting

In case of breach of requirements of the Ordinance, e.g., an incident of personal data leakage, both staff and teachers, and School Administration Department should report the incident to the Principal immediately.

Handling Personal Data in School

1. Personal Data of Teachers

The data can only be accessed by the Principal or the persons authorized by the Principal.

2. Personal Data of Students

A. Personal data

The data are kept in General Office and in WebSams

The right of access parts or all the data must be approved by the principal in prior

All staff should handle the data in accordance with the Personal Data (Privacy) School Guidelines

B. Students' marks & activities records

These data are kept in WebSams

The right of access parts or all the data must be approved by the principal in prior

All staff should handle the data in accordance with the Personal Data (Privacy) School Guidelines

Note not to expose the marks or other personal data of students to another student. For example, do not announce the marks of each student in the classes (except getting their consent in prior).

C. Comprehensive Social Security Assistance (CSSA) Scheme

The data are kept in General Office

Only the staff of General Office can have the right to access these data and it must be approved by the principal in prior

All staff should handle the data in accordance with the Personal Data (Privacy) School Guidelines

D. SEN students

The data are kept in General Office

The right of access parts or all these data must be approved by the principal in prior and the staff must sign before taking out the data for reference.

All staff should handle the data in accordance with the Personal Data (Privacy) School Guidelines