Tenby Schools, Malaysia
Personal Data Protection Policy: January 2014

The Personal Data Protection Act 2010 gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act gives the public a general right of access to information held by public bodies and outlines the requirements that must be followed when responding to requests. It also outlines reasons for withholding information, which are known as exemptions from the right to know.

Tenby Schools aims to fulfill its obligations under the Personal Data Protection Act 2010 by ensuring that anyone who processes personal information complies with the Act.

To ensure the implementation of the Act, a Data Protection Officer will be appointed in each Tenby School and within the Corporate Office.

The Act states that anyone who processes personal information must comply with eight principles, these are that personal information is:

- Fairly and lawfully processed and that the individual has given consent
- Processed for the specified purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with an individual’s legal rights
- Secure
- Not transferred to other countries without adequate protection

Security Measures In Place

The school has procedures in place to ensure appropriate use, disclosure and protection of personal data, including sensitive data relating to members of staff and students’ records. The school uses physical and electronic safeguards to ensure the security of data.

These include:

- Locks to filing cabinets
- Locks to doors, to offices, filing rooms and computer rooms
- Secure management of the holding and storage of keys
- Installation of anti-virus software
- Installation of firewall software/hardware
- Secure data backup procedures
- Good practice relating to passwords, clear screens, locking of computers
- Separate administration and teaching computer areas

D. Sinclair Final Version 28th January 2014
Personal Data Covered by the Act

This includes, but is not limited to:

- School admission and attendance registers
- Students' curricular records
- Annual returns to the relevant authorities
- Reports to parents on the achievements of their children
- Records in connection with students entered for public examinations
- Staff records, including disciplinary and payroll records
- Student disciplinary records
- Records of contractors and suppliers
- Personal information for teaching purposes (assessment data, teacher mark books)

Sensitive Data

Sensitive data can only be processed if the information has been lawfully and fairly obtained and that the subject has consented, sensitive data includes:

- Ethnic origin
- Political opinions
- Religious beliefs
- Other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health condition
- Alleged and/or criminal offence
- Proceedings or court sentence

The School's Data Protection Officer is responsible for deciding how any personal data is to be processed and ensuring that it complies with the Personal Data Protection Act 2010.

Access to Information

The second area covered by the Data Protection Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records. With regard to students, there are two distinct rights to information held by the school:

1. The subject access right – where a student has the right to a copy of his/her own information. Requests may also be made by a parent/guardian on behalf of his/her child. All students and parents are entitled to have their records disclosed to them on written request, unless it is obvious that they do not understand what they are asking for, or if disclosure would be likely to cause them or anyone else serious physical or mental harm.

2. Rights to the educational record – under the Act 2010 a parent/guardian has the right to access his/her child's educational
record.

All requests should be addressed to the Data Protection Officer at the relevant Tenby School. The request should be made in writing and describe the information to which access is required. If practicable and reasonable, the information will be copied or printed and posted to the person making the request. Arrangements can be made to view the information by an individual as an alternative. The School will comply with the request within a period of 14 working days.

There are certain circumstances, where access will be denied. This includes cases where the information might cause serious harm to the physical or mental health of the students or another individual or the request would entail releasing examination marks before they are officially announced.

When a student transfers to another Tenby school, the new school should be sent a completed transfer form and all educational records relating to the student, including copies of their student reports. When a student transfers to a new school other than Tenby Schools, all educational records relating to the student, including copies of their student reports should be provided to the parents/guardians.

**Charging**

Straightforward requests for information are provided free of charge. More complex requests will be charged; the school’s Data Protection Officer will provide details regarding charges on request.

**Sharing of Data and Student consent**

The interests of the student should remain paramount at all times. Whenever possible, students should be consulted and their wishes taken into account concerning the sharing of information about them. The exceptions to this are:

When there is a legal obligation to share information without the consent and/or knowledge of the student, e.g., child protection; when the student is deemed to be unable to make a competent decision concerning the sharing of information about them. In such instances, those who are responsible for the student should be consulted.

It should be made clear as early as possible that absolute confidentiality cannot be guaranteed if a student’s own safety or the safety of others is at risk. Where a member of staff believes that there is a risk to the health, safety or welfare of a young person or others, which is so serious as to outweigh the young person’s right to privacy, they should clearly explain this to the student and inform the Principal.

**Sharing data within the school**

Those responsible for sharing personal or confidential information about students or staff should work together to ensure that such sharing is handled in line with statutory guidance. Responsible staff should meet to discuss and
agree on what information should be shared, for what legal or proper purpose, to whom it should be shared and how much information should be reasonably disclosed. Sensitive data such as medical information on staff and students should not be displayed in 'public' areas where guests to the school may be admitted.

Who needs to know?

Potentially, those who work directly with students may need to be informed of confidential information. Those responsible for the running and administration of the school may also need to be informed. These include:

- Form Tutors
- Teaching Staff,
- Pastoral and Support Staff,
- Parents,
- Guardians or Carers,
- School Principals,
- School Board Members,
- Outside Agencies

Basis for sharing information

Information may be shared

- for information only (e.g. to ensure others may respond appropriately in the case of classroom management, potential problems)
- because action is required (e.g. to inform the Principal in the case of possible Child Protection issues)

Information should only be shared

- on a 'need to know' basis
- in accordance with legal requirements

Where an individual faces a conflict of interest about whether to disclose information or not

- the interests of the students take priority
- other staff who share the information should be consulted

When in doubt, information should not be shared unless

- there is a legal requirement to do so
- there is a clear benefit to the student to do so
- that the student will be protected from harm by the disclosure

Disclosure of Data - Staff

Personal data cannot be released to third parties without the individual's
consent, unless for specific reasons such as prevention or detection of crime, the health, safety and welfare of other employees or where disclosure is to protect the vital interests of the individual. Ideally, the individual's consent should be obtained in writing. If the school wishes to obtain personal data from a third party, e.g. an employee's medical records, the individual's permission should be requested and obtained.

All requests for disclosure should be submitted in writing on headed paper and given full reasons.

Accurate information should be given when supplying a reference for an employee or ex-employee.

Rights of Individuals

When the School requests personal data they must inform individuals as to why the personal data is being processed and to whom it is being disclosed. Personal data held by the school is reviewed and updated annually as necessary. Personal data is held by the school for seven years.

Personal information given in confidence must not be disclosed without consent. Employees should not be the subject of monitoring without good cause.

Individuals have the right to prevent processing, which is damaging or distressing to themselves or others, to prevent processing for direct marketing, ensure that no decision significantly affecting them is based solely on the automatic (electronic) processing of data relating to them e.g. assessing their performance at work. The individual also has the right to rectify, block, erase or destroy inaccurate data on application to the school.

Exemptions

Individuals are not entitled to have access to the following:

- References given by an employer
- Personal data processed for the purposes of management planning e.g. pay reviews, promotion Information about or provided by a third party where the third party could be identified and does not agree to a disclosure

Policy to be reviewed: January 2016

Signed on behalf of Tenby Schools:

Name (Principal/Director) [Signature]

Signed [Signature]

Date 10.02.14.

D. Sinclair Final Version 28th January 2014