Personal Data Protection Policy

Westlake International School

Westlake
International School

Approved by:	SLT
Ownership:	IT
Last reviewed on:	July 2021
Next review due by:	December 2021

Introduction

WIS needs to gather and use certain information about individuals.

These can include parents, students, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the organization's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures WIS:

- Complies with data protection law and follows good practice.
- Protects the rights of parents, students, suppliers, business contacts, employees and other people the organisation has a relationship with.
- How data is processed, stored and secured.
- Protects itself from the risks of a data breach.

Data protection law

The Personal Data Protection Act 2010 describes how organisations including WIS must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

Policy scope

This policy applies to:

- The head office of WIS
- All branches of WIS
- All staff and volunteers of WIS
- All contractors, suppliers and other people working on behalf of WIS

It applies to all data that the organization holds relating to identifiable individuals, even if that information technically falls outside of the Personal Data Protection Act 2010. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data protection risks

This policy helps to protect WIS from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the organization uses data relating to them.
- **Reputational damage.** For instance, the organization could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with WIS has responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that WIS meets its legal obligations.
- The **data Protection officer ,** is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data WIS holds about them.
    - Checking and approving any contracts or agreements with third parties that may handle the organization's sensitive data.
- The Head Of IT**,** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the organization is considering using to store or process data. For instance, cloud computing services.
- The **Principal,** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure branding initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their department head.
- **WIS will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the organization or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their department head or the **data protection officer** if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the **data protection officer** (DPO).

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer or on a desk unattended.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a DVD or external storage), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing service**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the organization's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to WIS unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Data must be **encrypted before being transferred electronically**. The IT department can explain how to send data to authorised external contacts.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data accuracy

The law requires WIS to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort WIS should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- WIS will make it **easy for data subjects to update the information WIS** holds about them. For instance, via the organization website or School Management system
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by WIS are entitled to:

- Ask **what information** the organization holds about them and why.
- Ask **what information** the organization will share with others.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the organization is **meeting its data protection obligations**.

If an individual contacts the organization requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the **data protection officer** at **dpo@westlakeschool.edu.my**.

The **data protection officer** will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Personal Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, WIS will disclose requested data. However, the **data protection officer** will ensure the request is legitimate, seeking assistance from the board and from the organization's legal advisers where necessary.

Providing information

WIS aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the organization has a privacy statement, setting out how data relating to individuals is used by the organization.

[This is available on request. A version of this statement is also available on the organization's website.]