Tohoku International School Data Protection Policy

Important Points:

Here are a few ways that you can protect data at Tohoku International School

Do:

- Use strong passwords and update them regularly.
- Use encryption when storing or sending sensitive data.
- Close or Lock your computer when you leave it anywhere.
- Be aware of phishing scams and suspicious emails or messages.
- Report any security incidents or suspected breaches immediately to the Tech Coordinator.
- Shred paper documents with any personal information.

Do Not:

- Use public Wi-Fi networks to access sensitive data.
- Share login credentials with anyone, and do not write them down or store them in an easily accessible location.

Scope

This policy applies to all data maintained or processed at TIS, including student education records, student work, employee records, financial information, disciplinary records, information on educational concerns, and any other sensitive or confidential data.

Philosophy

At TIS, we recognise that protection of data is important and that the members of our community have rights with respect to the personal data that we process.

During the course of our business and educational activities, we collect, store and process personal data. We endeavor to treat this data in accordance with legal safeguards and in a manner consistent with our Common Values.

All our staff members are required to comply with this Data Protection Policy when processing personal data as part of their role. Failure to comply with this policy may lead to disciplinary action.

The Leadership Team is responsible for ensuring compliance with this policy in their respective areas of responsibility.

This policy is overseen by the school's Data Protection Officer (dpo@tisweb.net).

Data Protection Terms

For the purposes of this policy, the following terms apply:

Data Controller is the organization that determines the purposes for processing personal data and the manner in which that processing is carried out. In most cases, Tohoku International School is the Data Controller of the personal data it collects and uses as part of its business and educational activities.

Data Processor is the organization or person that processes personal data on our behalf and in accordance with our instructions, such as suppliers and contractors. Our staff members are not Data Processors.

Data Subjects are all individuals about whom we hold personal data.

Personal Data are any information relating to a living individual who can be identified from that information or from any other information we may hold. Personal data can include names, identification numbers (including MyNumber), addresses (including IP addresses), dates of birth, financial or salary details, education background, job titles and images. It can also include an opinion about an individual, their actions or their behavior. Personal data may be held on paper, in a computer or any other media.

Special Category Data are more sensitive, and include information revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs. It may also include data concerning health (physical and/or mental health), or biometric information where that data is used to uniquely identify a person. This term also refers to data relating to criminal convictions or related proceedings obtained through third-party background screening of prospective employees.

Processing means any activity which is performed on personal data or special category data. It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction of data.

Data Classification

Data should be classified according to sensitivity or criticality, based on its potential impact on the school or individuals if it were to be lost, stolen, or accessed without authorization. The school will use the following classifications:

- **Public**: Data that is intended for public release and has no sensitivity or confidentiality requirements.
- **Internal**: Data that is intended for internal use and is not public-facing. This data may include employee records or internal communications.
- **Confidential**: Data that is sensitive and should be protected from unauthorized access or disclosure. This may include student education records, financial information, or health information.
    - Regarding student education records -
        - Parents and students have the right to review school records including grades and disciplinary records. Parents and students do not have the right to modify these records.
        - Modifications can be requested by a student or parent, but the school may use its discretion in approving modifications and should only modify records in order to correct factual errors.
        - School records, including transcripts, disciplinary records, and IEPs, may be provided by TIS to another school or school district when a student is transferring to that school. In this case, TIS will make a reasonable effort to notify the parent and/or student of the provision.
        - Student Records or other information may be provided to third parties in order to comply with the laws of Japan. Examples would include official requests by police or welfare officials.

Access Controls

Access to school data should be granted on a need-to-know basis, with the least privilege principle applied. Access should be regularly reviewed and revoked when it is no longer needed. The school will implement appropriate authentication and access control measures, including password policies, two-factor authentication, and user account management.

- Access to Google drives and folders, email accounts, and social media should be reviewed regularly by the IT Coordinator.

Guidelines for Data Access

Specific Permissions

	Types of Data								
	Operational finance Data	Employee Salary, Benefit, Insurance and Tax Data	Student Payment	Employee Health	Student Health	Policy Level Documents	Curriculum Documents	Classroom Communications	Student Produced work

Principal	✔	✔	✔	✔	✔	✔	✔	✔	✔
Office	✔	✔	✔	✔	✔	✔			
Senior Leadership			✔	✔	✔	✔	✔	✔	✔
Team Leaders						✔	✔	✔	✔
Teachers						✔	✔	✔	✔
Part-time Staff									✔

Underlying Principles

Tohoku International School believes that:

- Personal data should only be used to conduct needed business or educational activities, and should never be used for the personal benefit of staff.
- Data should be kept up-to-date and accurate, and deleted timeously when no longer needed.
- Breach of data protection can affect the rights and freedoms of data subjects and this should be avoided as much as possible.

Tohoku International School is committed to:

- Taking all reasonable steps to ensure that any personal data collected is kept secure, and only accessible to authorized persons or organizations.
- Complying with all relevant privacy laws, including the Act on Protection of Personal Information (APPI), the My Number Act, and the European Union General Data Protection Regulation (GDPR), where applicable.
- Communicating transparently with data subjects in cases where their personal data may have been compromised.

Data Protection Roles

It is the responsibility of all employees and other individuals who handle school data to ensure that it is protected from unauthorized access, disclosure, or modification.

The following staff members, hereafter referred to as the Data Protection Committee, are responsible for ensuring compliance with this policy:

- Principal: Ms. Kathryn Simms principal@tisweb.net
- Office staff: Ms. Yukiko Kawaguchi ykawaguchi@tisweb.net

- Data Protection Officer: Mr. Zane Clifford dpo@tisweb.net

Data Protection

The school will take appropriate measures to protect data from loss, theft, or unauthorized access. This includes:

- Seeking approval for apps and tech to be used in the classroom. This is especially important in the case that an account must be made for each student. (See COPPA "Children's Online Privacy and Protection Act).

- Encrypting sensitive data in transit and at rest

    - Data in transit refers to the movement of digital data over a network or between two devices, such as between a user's computer and a server or between two servers. This data may be transmitted over a wired or wireless network and can include various types of information, such as email messages, file transfers, or website requests. It is important to ensure the security of data in transit to prevent unauthorized access or interception by third parties. This can be achieved through the use of encryption and other security measures.
        - The two most important security measures for most users are strong passwords and caution against phishing or other data leaks.
    - Data at rest refers to digital data that is stored or archived in some form of electronic storage device or medium, such as a hard drive, solid-state drive, USB flash drive, or a cloud storage service. This data is typically not actively being accessed or transmitted over a network, but rather is stored for later use or reference. Examples of data at rest may include files, databases, emails, or backup copies of data. Security can be achieved through the use of access controls, encryption, and other security measures.
- Storing data on our Google Drive in appropriate shared drives or files
- Regularly updating software and systems to address security vulnerabilities
- Implementing appropriate antivirus and malware protection
- Data Retention and Disposal - Data should be retained only for as long as necessary to meet the school's operational or legal requirements. When data is no longer needed, it should be disposed of securely using appropriate methods, such as shredding or electronic destruction.

Procedure in the event of Data Breach

The procedure to be followed in the event of a data breach will consist of the following 5 steps:

1. Initial Reporting
2. Containment
3. Assessment
4. Report to Personal Information Protection Commission (PPC)
5. Accountability and Response

At each point in the process, a log of events and actions taken will be kept.

Initial Reporting
When a data breach occurs, or a staff member has reason to believe that such has occurred, they should bring the matter to the attention of the Data Protection Officer by emailing dpo@tisweb.net. The Data Protection Committee will meet to decide whether to further investigate the report.

Containment
If the report is found to be credible, a determination must be made as to if the breach is ongoing or has been contained. Containment procedures may include, but are not limited to: isolating affected systems, changing of passwords, scanning for malicious software, review of CCTV footage and communication with law enforcement.

Assessment
Once the breach has been contained, the Data Protection Committee will meet again to determine the severity of the breach, and whether a report to the PPC is required. Reporting is mandatory in the case where a data breach involves or is likely to involve sensitive Personal Data, there is risk of financial damage, or where the data breach involves more than 1000 Data Subjects. (Education Privacy Handbook Japan v2.0, 9ine / Japan Council of International Schools)

- Where these conditions are not met, the data breach will be recorded in the log as a Non-Reportable Breach
- In the case where the above conditions are met, the data breach will be recorded in the log as a Reportable Breach. PPC guidelines state that an initial report must be made within 3 to 5 days, with a more detailed report following within 30 days. Events will then proceed according to instructions given by the PPC.

Accountability and Response
All relevant information about the breach will be recorded in the log, including

- A summary of the event
- Any actions taken to contain the breach

- Whether the breach was considered Non-Reportable or Reportable
- What actions have been taken to ensure that a similar breach does not reoccur.

Data Shared with Third Parties

The following are considered to be Third Parties, which processes personal data on our behalf and in accordance with our instructions. Links are included to the data protection policy of each.

- Alma
- Toddle
- Class Dojo
- Google

Use of CCTV

TIS uses Closed Circuit TV (operated by *Unifi Protect*) as a security measure for the following purposes:

- To maintain the security of our students, staff and visitors to the school
- To resolve disputes which may arise in the course of disciplinary proceedings
- To prevent and detect crime such as vandalism, trespassing or theft
- To assist law enforcement in preventing, detecting and prosecuting crime

Footage may be viewed by the Leadership team and Data Protection Officer for purposes mentioned above.

Cameras are located only in public areas, such as corridors and offices and are positioned to view entrances/exits. Cameras are not used in areas where there is an expectation of privacy, such as classrooms or restrooms. The camera locations are as follows:

- Main Building, First floor
    - Hallway 1 (Room 11-13)
    - Hallway 2 (Room 14,15)
    - Shokuguchi (Main Door)
    - Shokuguchi (Side Door)
- Main Building, Second floor
    - Library
    - Bridge to TIS
    - Hallway(Room 21-23)
- Main Building, Third floor
    - Hallway (Room 31, 32)
- Building 1, First floor
    - Hallway
    - Front Entrance

- Building 1, Second floor
    - Hallway
- Playground (Outside)

The data collected by the cameras is stored on the TIS server for a period of 31 days, after which it is deleted.

Review of recorded security camera footage will occur only when there is a claim of an injury or an incident that raises safety or security concerns. For the protection of privacy, only staff investigating an incident, as designated by the Principal, may have access to security camera footage. At the discretion of the Principal, footage may be shown to parents or students if required by the situation. A note stating that stored footage was reviewed, and by whom, should be added to the incident report or other documentation.

The Data Protection Committee may allow appropriate law enforcement agencies to view or remove security camera footage where this is required for the detecting or prosecution of crime.

The Data Protection Committee may also release security footage to a third party where it is required for legal proceedings or has been requested by way of a court order.

The DPC will maintain a record of all disclosures of security camera footage.

Contact Details

Any questions or concerns relating to this policy should be directed to our Data Protection Officer at dpo@tisweb.net.

Conclusion

This school data security policy is intended to provide guidance on how the school handles sensitive data and to ensure that it is protected from unauthorized access or use. The policy should be regularly reviewed and updated to reflect changes in technology, regulations, or best practices.

Documentation Referenced in the Preparation of this Policy

Family Educational Rights and Privacy Act (FERPA) rights of Parents: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/A%20parent%20guide%20to%20ferpa_508.pdf

Children's Online Privacy Protection Act (COPPA):
https://www.ftc.gov/system/files/documents/plain-language/coppa-plain-language.pdf
Payment Card Industry Data Security Standard (PCI DSS):
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
Health Insurance Portability and Accountability Act (HIPAA):
https://www.hhs.gov/sites/default/files/hipaa-simplified-privacy-rule-8-10-2016.pdf