SIS POLICY MANUAL

450-1: PERSONAL DATA PROTECTION PRACTICES

CREATED	EFFECTIVE ON	REVIEWED	NEXT REVIEW
Mar 12 2024	1st May	Yearly	May 2025

Introduction

This document outlines SIS's data protection practices, emphasising educators' responsibilities and the prudent handling of all student data, including student photographs. Compliance with the *General Data Protection Regulation (GDPR) is paramount for safeguarding the privacy and security of personal data within our academic setting.

Understanding GDPR

The GDPR establishes rigorous principles and obligations for personal data protection within the European Union (EU). Educational institutions, as data controllers and processors, must ensure that personal data is:

- Processed lawfully and transparently.
- Collected for specific, legitimate purposes.
- Adequate and relevant.
- Accurate and up-to-date.
- Stored securely.
- Protected against unauthorised or unlawful processing.

Data Protection Officer (DPO)

The appointed SIS DPO is the Schoolwide Data Lead.

The DPO plays a vital role in GDPR compliance:

- **Advisory Role:** Advises the institution and staff on GDPR obligations.
- **Compliance Monitoring:** Regularly reviews compliance, including assigning responsibilities and training staff.
- **Authority Cooperation:** Serves as the contact point for supervisory authorities and assists with processing inquiries.

Teacher Responsibilities

Teachers interact with data frequently and have specific responsibilities:

- **Legal Understanding:** General comprehension of GDPR principles and their application to student data.
- **Confidentiality Maintenance:** Ensure the privacy and security of student information, including academic records and sensitive data.
- **Incident Reporting:** Promptly report data breaches or security incidents to the DPO and IT Manager (Helpdesk).

Use of Social Media

Guidelines for responsible social media use include:

- **Informed Consent:** During enrolment and re-enrolment, obtain explicit consent from students or guardians to post personal data, including photographs.
- **Educational Focus:** Use social media for educational purposes, fostering positive interactions and respecting student privacy.
- **Content Monitoring:** Regularly review social media content to ensure compliance and address inappropriate or unauthorised postings.
- **Content Approval:** DPO is to review Social Media content regularly to ensure it is compliant with Data Protection Practices

Student Photographs

Specific considerations for managing student photographs are crucial:

- **Usage Policy:** Establish a policy outlining the use, storage, and sharing of photographs in accordance with GDPR.
- **Limited Access:** Restrict access through password protection to photographs, including on SmugMug, to authorised personnel only, using technological measures to prevent unauthorised access.
- **Anonymisation:** Utilise anonymised or de-identified images to minimise privacy risks, especially for broader purposes. This means only using the first name when publishing images.

Rights of Data Subjects

Upholding the rights of students and guardians includes:

- **Transparency:** Provide clear information on data usage, storage, and protection renewed annually as part of re-enrolment.
- **Changes: If a student's name changes, it** must be changed centrally through the school registrar and often with HoS approval.
- **Consent Withdrawal:** Enable data subjects to revoke their consent easily.
- **Data Portability:** Allow data subjects to request and receive their data.

Open Apply (enrolment platform) Statement

In its collection and use of personal information, from now on called "personal data", about students, parents and other individuals in contact with the school, SIS will act to ensure that such personal data is dealt with lawfully and securely in accordance with current best practice in protecting data however it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

Incident Response

Effective incident response mechanisms are essential:

- **Immediate Action:** Implement procedures for prompt detection, investigation, and containment of data breaches.
- **Incident Documentation:** For accountability and audit purposes, maintain records of personal data breaches, their impact, and corrective actions taken.

* The General Data Protection Regulation (GDPR) is a European Union (EU) regulation that sets out data protection and privacy requirements for organisations that process the personal data of individuals within the EU. Although the GDPR does not apply in China, it can still impact organisations in China that process the personal data of EU residents. For example, if SIS enrols EU residents, the EU monitors their behaviour and must comply with the GDPR.

Many Chinese companies voluntarily adopt the GDPR as a best practice to demonstrate their commitment to data protection and privacy.