Approved by: Principal	Date: 30 January 2026

Last reviewed on:	Date: 26 January 2026

Next review due:	Date: 22 June 2026

#	Description of Changes	Rev. No	Date of Issue
1	First Issue	00	21 June 24

ICS Vision
The "School of Choice" inspiring, challenging and empowering a 21st century learning community through an ethical and innovative education system.

ICS Mission
Provide a safe, friendly learning environment where lifelong learners follow an international curriculum which promotes academic excellence and nurtures key values and competences in our global minded, future leaders.

Introduction

At International Community School (ICS), we recognize the importance of protecting personal data and ensuring digital safety in an increasingly connected world. Our commitment to safeguarding the privacy and security of all members of our community is central to our operations. This policy outlines how ICS complies with data protection regulations, including the Federal Decree Law No. (45) of 2021 on the Protection of Personal Data, and how we manage the use of digital technologies in line with the Abu Dhabi Department of Education and Knowledge (ADEK) Digital Policy.

Purpose

This policy is designed to ensure that:

- ICS adheres to all applicable data protection laws and digital safety standards.
- All personal data collected, stored, and processed by ICS is handled securely and lawfully.
- Digital technologies are used responsibly and safely by students, staff, and other members of the school community.
- The school has clear procedures for managing data breaches, digital incidents, and cybersecurity threats.
- There is a clear framework for the roles and responsibilities of staff members in relation to data protection and digital safety.

Definitions

Personal Data
Any information relating to an identified or identifiable individual. This includes names, identification numbers, location data, online identifiers, and other factors specific to an individual's physical, physiological, genetic, mental, economic, cultural, or social identity.

Special Categories of Personal Data
Sensitive data requiring additional protection, including information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (used for identification), health, and sex life or sexual orientation.

Processing
Any operation performed on personal data, including collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying it.

Data Subject
The individual whose personal data is processed.

Data Controller
The person or organization that determines the purposes and means of processing personal data.

Data Processor
A person or entity that processes personal data on behalf of the data controller.

Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

Digital Device
Any electronic device used for communication, computing, or data storage, including smartphones, tablets, laptops, and desktop computers.

Cybersecurity Incident
A breach that threatens the confidentiality, integrity, or availability of information systems or sensitive data.

Roles and Responsibilities

Governing Body
The Governing Body holds overall responsibility for ensuring ICS complies with all relevant data protection and digital safety obligations. It oversees the implementation of this policy and ensures the school is adequately resourced to meet its legal requirements.

Principal
The Principal acts as the representative of the data controller, overseeing the day-to-day management of data protection and digital safety at ICS. The Principal ensures that staff are aware of their responsibilities and that the school's digital infrastructure is secure.

Sr. IT Officer (SIO)
The SIO is responsible for monitoring ICS's compliance with data protection laws and overseeing the implementation of this policy. The SIO provides guidance on data protection issues, manages data breaches, and reports to the Governing Body on data protection matters. The SIO is responsible for ensuring the digital safety of students and staff. This includes implementing the school's digital strategy, managing digital incidents, and liaising with ADEK on matters related to digital safety and cybersecurity.

Staff Members
All staff members are responsible for following the data protection and digital safety guidelines set out in this policy. This includes ensuring that personal data is processed lawfully, securely, and in accordance with this policy. Staff are also responsible for reporting any digital incidents or data breaches to the SIO.

Students and Parents
Students and parents are expected to use digital devices responsibly and adhere to the school's digital safety guidelines. Parents are responsible for monitoring their children's use of digital devices outside of school hours to ensure safe and appropriate behavior.

Data Protection Principles

ICS adheres to the following data protection principles:

- **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully, fairly, and transparently.
- **Purpose Limitation**: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data Minimization**: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy**: Personal data must be accurate and kept up to date.
- **Storage Limitation**: Personal data must be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data is processed.
- **Integrity and Confidentiality**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Collecting and Processing Personal Data

ICS will only collect and process personal data where there is a lawful basis for doing so. These bases include:

- Processing is necessary for the performance of a contract to which the data subject is a party.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary to protect the vital interests of the data subject or another individual.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- Processing is necessary for the legitimate interests of ICS or a third party, provided these interests are not overridden by the rights and freedoms of the data subject.
- The data subject has given consent to the processing.

Digital Strategy and Oversight

ICS has developed a comprehensive digital strategy that outlines our goals for the use of technology in education. The strategy includes:

- **Digital Competency Goals**: Defined digital competencies for students by grade level, integrated into the curriculum to ensure students are proficient in digital skills.
- **Infrastructure Development**: Plans for the development, procurement, and implementation of digital infrastructure, including hardware, software, and assistive technology for students with additional learning needs.
- **Cybersecurity Measures**: Mechanisms to ensure the security of ICS's digital systems, including multi-factor authentication, encryption, and regular security audits.
- **Staff Training**: Ongoing training for staff on digital safety, data protection, and the use of digital technologies in education.
- **Monitoring and Evaluation**: Regular reviews of the digital strategy's effectiveness, including assessments of student digital competency and the security of the school's digital infrastructure.

Responsible Usage and Digital Safeguarding

ICS is committed to promoting responsible digital behavior among all members of the school community. This includes:

- **Responsible Usage Policies**: Clear guidelines for the responsible use of digital devices, software, and networks by students, staff, and visitors. This includes restrictions on the use of personal devices on school premises and guidelines for the use of social media.
- **Digital Safeguarding Programs**: Education programs to raise awareness of online risks, such as exposure to inappropriate content, cyberbullying, and digital addiction. These programs include age-appropriate lessons on digital citizenship and online safety.
- **Monitoring Systems**: Tools and procedures to monitor student internet use on school devices and networks, ensuring compliance with responsible usage policies and identifying potential risks.

Data Security and Storage

ICS implements robust data security measures to protect personal data from unauthorized access, loss, or destruction. These measures include:

- **Access Control**: Role-based access controls to ensure that only authorized personnel can access sensitive data.
- **Encryption**: Use of encryption for data in transit and at rest to safeguard personal information.
- **Data Backup and Recovery**: Regular backups of critical data, with secure storage and a robust disaster recovery plan in place to minimize downtime in the event of a data breach.
- **Physical Security**: Secure access to physical servers, networking equipment, and other critical infrastructure to prevent unauthorized access.

Data Breach Management

In the event of a data breach, ICS will follow a clear procedure to manage and mitigate the impact:

- **Immediate Reporting**: Any staff member who identifies or causes a potential data breach must immediately notify the SIO.
- **Breach Containment**: The SIO will work with relevant staff to contain the breach and minimize its impact.
- **Risk Assessment**: The SIO will assess the potential consequences of the breach and determine whether it needs to be reported to ADEK.
- **Notification**: If required, the SIO will notify ADEK within 72 hours of the breach, providing a detailed report of the incident and the steps taken to mitigate its impact.
- **Review and Prevention**: Following a breach, the SIO and Principal will review the incident to identify lessons learned and implement measures to prevent future breaches.

Cybersecurity

ICS is committed to maintaining a secure digital environment for all members of the school community. Our cybersecurity measures include:

- **Multi-Factor Authentication**: Implementing multi-factor authentication for critical services to enhance security.
- **Next-Generation Firewalls**: Deploying advanced firewalls and intrusion detection/prevention systems to protect against unauthorized access.
- **Endpoint Protection**: Ensuring that all school-managed devices have up-to-date antivirus and anti-malware software.
- **Incident Response Plan**: Developing and regularly updating an incident response plan to address cybersecurity breaches promptly and effectively.

Data Protection by Design and Default

ICS incorporates data protection principles into all our data processing activities. This includes:

- **Privacy Impact Assessments**: Conducting privacy impact assessments for new projects or technologies that may pose a high risk to individual privacy.

- **Staff Training**: Providing regular training for staff on data protection law, this policy, and best practices for handling personal data securely.
- **Documentation**: Maintaining detailed records of data processing activities, including data categories, processing purposes, and security measures in place.

Digital Communications

ICS has established clear guidelines for digital communications, including the use of social media and the publication of digital content:

- **Digital Media Policy**: Ensuring that any digital media involving students is created and published only with parental consent and that all digital content is stored securely.
- **Social media**: Guidelines for the use of social media by staff, including privacy settings, content appropriateness, and the prohibition of using personal accounts to communicate with students or parents.
- **Email Communication**: Prohibiting the use of personal email accounts for school-related communication to ensure data security.

Compliance

ICS is committed to full compliance with all applicable data protection and digital safety regulations. This policy will be reviewed annually to ensure it remains up to date with current laws and best practices. Non-compliance with this policy may result in disciplinary action and legal accountability.

Linked Policies

This Digital and Data Protection Policy is interconnected with several other ICS and ADEK policies, ensuring a comprehensive approach to digital safety and data protection. These linked policies include:

- Safeguarding Policy
- Acceptable Use Policy
- Child Protection Policy
- Student Protection Policy
- Inclusion Policy
- Student Behavior Policy
- Records Policy
- Student Mental Health Policy