DATA PROTECTION POLICY

Scholars Indian Private School highly prioritize its Data Protection Policy, which is a set of principles, rules and guidelines that ensures how your personal data will be protected by the organisation.

The policy applies to all school staff members, the Board of Management, parents, students and to all other individuals who come in contact with the school. School collects personal data and uses personal information about staff, pupils and parents and in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Purpose

The terms, conditions and statements within this policy are intended to ensure that personal information about staff is dealt with correctly and securely. This will apply to information regardless of the way it is collected, used, recorded, stored, and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing, and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

We examine and analyse the personal data we hold in order to

1. To be able to provide secure access of data.
2. Document our data protection procedures
3. To enhance accountability and transparency.

Data Protection Principles

The school management is the data controller of personal data relating to past, present and future staff, parents and other members of school community. We comply with the principles set out in the Data Protection Acts of UAE government.

- Personal data shall be processed fairly and lawfully
- Personal data shall be adequate, relevant, and not excessive
- Personal data shall be accurate and where necessary, kept up to date
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes (if time sensitive documents)
- Personal data shall be kept secure

General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals the purpose of information collected.
- Inform individuals when their information will be shared, and why and with whom it will be shared.

- Check the quality and the accuracy of the information it holds.
- Ensure that information is not retained for longer than is necessary.
- Ensure that when obsolete information is destroyed, that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Share information with others only when it is legally appropriate to do so.
- Ensure our staff is aware of our policies and procedures.

Actioning an Access Request

Any individual has the right of access to information held about them.
If you make an access request, and if we do hold information about you, we will:

- Give you a description of it
- Explain where we got it from, if not from you
- Give you a copy of the information
- Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.
  If you would like to make an access request to your data in our school's management system, please contact our Administrative Officer

The Personal Data We Hold and Why We Use This Data

Personal data is held by the school about those employed or otherwise engaged to work at the school. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit all school employees by:

- Improving the management of school workforce data across the sector
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up
- Informing the development of recruitment and retention policies
- Allowing better financial modelling and planning
- Enabling ethnicity/diversity

This information includes from staff for appointment:

- Contact details, identification documents
- Characteristics such as ethnic group
- Employment contract and remuneration details
- Qualifications
- Absence information
- Financial records
- Photos and video recordings for events
- CCTV records captured in the school

This information includes from parents and students for admission procedure:

1. Passport copy with valid visa page
   a. Child
   b. Both parents
2. Passport size photos-3 Nos
3. Emirates ID card copy and Original
4. Vaccination card copy
5. Birth certificate copy
6. Transfer Certificate
7. Copy of Report Card
8. Continuation Certificate from current school

Our Legal Basis for Using This Data

We only collect and use staff personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation to ministerial departments such as immigration/MOE/MOH/ICA/MOI/MOHRE/
- We need it to perform an official task in the public interest.

Collecting Information

While the majority of information we collect about staff is mandatory, there is some information that can be provided voluntarily.
Whenever we seek to collect information, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying. If it is optional the employee has the right to provide or not. We will explain the possible consequences of not complying.

How We Store Data

We keep personal information about staff while they are working at school. We may also keep it after their service to school for future recommendation or reemployment if this is necessary in order to comply with our legal obligations. Also this information is not shared after the completion of service at school without expressed permission from the previous employee.

Data Sharing

We do not share information about staff with any third party without consent and knowledge unless the law and our policies allow us to do so.
Where it is legally required or necessary (and it complies with data and privacy protection law) we may share personal information about staff with:

- Ministry of Education (MOE)

- Examining bodies (for example and noted limited to TIMSS, PISA, EMSAT, ASSET, PIRLS)
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Ministry of Health (MOH)

Where it is legally required or necessary (and it complies with data and privacy protection law) we may share personal information about parents and students with:

- Ministry of Education (MOE)
- Ministry of Health (MOH)
- Examining bodies (for example and noted limited to TIMSS, PISA, EMSAT, ASSET, PIRLS)

Registration with MOE and MOL for Private Schools

We are required to provide information about staff to the MOE and MOL as part of statutory data collections.

Transferring Data Internationally

Where we transfer personal data to a country or territory outside the UAE, we will do so in accordance with data and privacy protection law and with the consent and knowledge of the employee.

Other Rights

Individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause damage
- Object to being used to send direct marketing
- Update personal data

Complaints

We take complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint, please contact our Finance Controller.

Related Links:

Data and privacy protection in the UAE
Data protection laws - The Official Portal of the UAE Government

AGREEMENT FORM

By signing this form and sending it to Administrative Officer you agree to the terms of the Staff Data Protection Policy.

All fields are required.

Staff Full Name : _____
Signature : _____
Date : _____

Technical Security

This aspect describes the ability of the school to understand and ensure reasonable duty of care regarding the technical and physical security of administrative and curriculum networks (including Wi-Fi) and devices and the safety of its users.

Securing Our Devices and Networks Both Online and Offline:

1. Secured website access (SSL is added).
2. All data are protected. Nobody can copy or download any content or files from the school website.
3. Back up of all data are taken on a regular basis.
4. Antivirus and Anti-malware protection is done and updated regularly.
5. Old computers' hard drives are made unreadable.
6. Operating system is installed, updated and regularly
7. Software updates are automated.
8. Wireless network is secured.
9. Separate Internet and Wi-Fi password is enabled for each block
10. Computers are turned off as soon as work is over.
11. IPV6, IPV4, IP sac pass through firewall protections are enabled
12. More of passphrases are used than passwords.
13. File and media sharing is disabled when not required.
14. Students are given access to school website and portal access all E-learning content, attendance, examination mark list and report card.

Data Protection for CCTV camera

CCTV cameras are implemented in all the building blocks of the school. It is controlled, protected and monitored by IT coordinator on regular basis. CCTV footages are backed up in the server and are maintained for a period of 4 months.

Filtering strategies

This aspect covers the school's ability to manage access to content across its system and monitor activity to safeguard users. In each device, option to block unwanted data is available in firewall and is enabled. We have used level filtering for accessing school data in the admin network.

All our data is secured and maintained in administration network of our school. Teachers and students have no access to this network.

Backup

Backup refers to copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event. All data related to parents, students and software are kept as backup regularly both in external and internal storages.

Purpose of backup and its importance

With an ever increasing data on school's network, along with larger number of people storing more important data than ever before and due to the rise in malware, virus and ransom ware attacks, Scholars make sure that data is safely backed up at an accurate rate.

Restore or recovery

A true test of backup success is termed as restore and we have made sure all our data backup is restored properly and accurately on a regular and timely basis.

Our Commitments

In a school, the owner of the backup process is the Network Manager (IT Coordinator) and the owners of the data are typically the senior leadership team, the staff, the learners and parents.

Our Network Manager is inevitably familiar with the day-to-day problems of managing large amounts of data across the complex network.

Typically, we have a service level agreement (SLA) that would define all aspects of the IT department's interaction with the school at large, allowing for both the IT team and its clients, be it the school's management team, the teaching staff or the learners, to understand and agree the levels of support available.

Understanding the nature of data

Rather than treating all your data as the 'same', we categorise it. Good reasons for doing this include:

- As your data grows, you can ensure that the backups are completed in the most efficient way.
- When storing data, it will allow different levels of data security and retention to be applied.

How long data has to be retained

Understanding how long data is to be kept is important and will have a big impact on the sizing of your backup solution. Defining different retention periods for different types of data will allow the data owners to understand how long data is retained and allow you to optimise the use of backup resources. Some data may need to be kept for a longer period of time such as schools' financial data.

A level of expectation is set within our school of how long it is reasonable to expect a user to ask for a deleted file to be restored, and that length of time would be your retention. Once you have your list of categories, you may decide, in the first instance, that the majority of these can be treated in the same manner. As time progresses you may choose to subsequently assign a lower level of backup service to different categories.

Category 1. Data – Information that changes on a regular basis.

- Network operating system and configuration data.

Category 2. Data – Information that changes on a regular basis and has to be retained.

- User data; shared areas, pupil / staff individual
- Your school management information.

Category 3. Data- CCTV Footage

- Back up is done on a daily basis by external source and is maintained for 4 months.

Backup software

- Microsoft Windows Server Backup is used.
- Software is secure and protected**.**

Backup storage criteria

- We always ensure that your backup data is removable
- We always locate your backup data away from the original source.
- We always store media in accordance to the manufacturer's guidelines
- Back up storage is done in our server and also on an external hard disk.
- A copy of backup data is maintained by our software company, Orison.

Implementation Arrangements, Roles and Responsibilities

The Board of Management and Principal implements the Data Protection Policy, ensuring that staff who handle or have access to Personal Data are familiar with their data protection responsibilities. IT Coordinator is responsible for day to day management and security of all levels of data.

Reviewing and Evaluating the Policy

The policy will be reviewed and evaluated as needed. Ongoing review and evaluation will take cognizance of changing information or guidelines. The policy will be revised as necessary on the basis of review and evaluation and within the framework of school planning.

Adopted: April, 2020 **Reviewed and updated: April, 2023**

Hameed Ali Yahya K. M.
Principal