DATA PROTECTION POLICY

2020-2021

المدرسة الهندية العالمية الخاصة
INTERNATIONAL INDIAN SCHOOL

Reviewed & Updated: Term2, September 2020
Next review : March 2021
Prepared by School Council Members

المدرسة الهندية العالمية الخاصة
INTERNATIONAL INDIAN SCHOOL
P.O. BOX 5665, AJMAN, U.A.E | T : +971 67408333 | info@iisajman.org | www.iisajman.org

DATA PROTECTION POLICY

INTRODUCTION

International Indian School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the school 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.

This policy is intended to ensure that personal information is dealt with correctly and securely. It 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.

SCOPE & OBJECTIVE

This is a policy that applies to all Users and all Systems.
“Users” are everyone who has access to any of the school's IT systems. This includes permanent employees and also temporary employees, parents, students, contractors, agencies, consultants, suppliers, customers and business partners.
“Systems” means all IT equipment that connects to the School network or access school applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

What is Personal Information?
Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

POLICY

All student, employee, and organization data (International Indian Schools Data) is the property of the International Indian School.

If data on the school's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information. Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-school system any information that is designated as confidential, or that they should reasonably regard as being confidential to the school, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with the school's safe password policy.

International Indian Schools Data should not to be shared with a third party, including parents or community residents, unless authorized to do so in the performance of their regular duties.

Users who are supplied with computer equipment by the school are responsible for the safety and care of that equipment, and the security of software and data stored on other school systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated

purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the school's systems by whatever means and must report any actual or suspected malware infection immediately.

BACKUP AND DISASTER RECOVERY POLICY

International Indian School critical servers are backed up automatically by Imperis on regular intervals. IT personnel regularly monitor and verify the backup process and files. In case of a server failure a new server can replace the existing one by restoring the Backup on the new server. Verification and monitoring process is in place and quarterly backups are restored and verified.

A centralized antivirus system is functional at International Indian School to tackle the viruses and Trojans. Gateway firewalls is also up and running in order to secure the internet and email communication. The firewall works to prevent the users from watching unintended materials, torrent downloading etc. As per the levels set by the administration some of the users have the rights over some areas of the internet for educational and research purposes.

Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above.

All concerns, questions, suspected breaches, or known breaches shall be immediately reported to Data protection Officer.