## POLICY COMMITTEE MEMBERS

- **CEO – ACADEMIC DIVISION**
- **DEAN ACADEMICS**
- **PRINCIPAL**
- **ADMIN OFFICER**
- **SOFTWARE ANALYST- CORPORATE**
- **SCHOOL IT ADMINISTRATOR**
- **INFORMATICS HOD**
- **HR COORDINATOR**
- **SCHOOL COUNSELOR**
- **TEACHER REPRESENTATIVES**

**APPROVED BY**

**PRINCIPAL**

**SCHOOL PERSONAL DATA HANDLING**

Recent publicity about data breaches suffered by organizations and individuals continues to make the area of personal data protection a current and high profile issue for schools, academies and other organizations. It is important that the school has a clear and well understood personal data handling policy in order to minimize the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorized or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organizational reputation
- schools/colleges are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school will want to avoid the criticism and negative publicity that could be generated by any-personal data breach
- the school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation
- It is a legal requirement for all schools to have a Data Protection Policy and be able to demonstrate compliance with data protection law.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in the school but also from remote locations. It is important to stress that the data protection laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review their policy, in the light of pertinent local/external regulations and guidance and changes in legislation.

**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. It is the responsibility of all members of the school community to take care when handling, using or transferring personal data, that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the School head. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the relevant school policy which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance

**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.

**PERSONAL DATA**

The school and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is information that relates to an identified or identifiable living individual This will include:

- personal information about members of the school community – including students/pupils, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- curricular / academic data e.g. class lists, student/pupil progress records, reports, references
- professional records e.g. employment history, taxation and insurance records, appraisal records and references

- any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

**SECURE STORAGE OF AND ACCESS TO DATA**

The school ensures that systems are set up so that the existence of protected files is hidden from unauthorized users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords made up from a combination of simpler words and must ensure all passwords comply with the school's safe password policy. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data (desktops and laptops) should be secured with a lock-on-idle policy active after at most 5 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

All paper based personal data must be held in lockable storage, whether on or off site. 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 Iperius 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 are 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.

**SECURE TRANSFER OF DATA AND ACCESS OUT OF SCHOOL**

The school recognizes that personal data may be accessed by users out of school or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorized premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorized user from outside the organization's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software

**DISPOSAL OF DATA**

The disposal of personal data, in either paper or electronic form,is conducted in a way that makes reconstruction highly unlikely. Electronic files are securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated. A Destruction Log is kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

**DATA BREACHES**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

The school have policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

**TRAINING & AWARENESS**

All staff should receive data handling awareness/data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / training sessions
- Day to day support and guidance from System Controllers

**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 the Data Protection Officer.

**REVIEW**

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 1 year. The policy review will be undertaken by the Principal, or nominated representative.

**CONTACT**

If you have any queries or concerns regarding this policy then please contact itsupport@iisajman.org