Approved by: Steve Brown on 01/01/2019

POLICY STATEMENT

Data Protection

VERSION NUMBER:	**1.0**
THIS VERSION:	
PREVIOUS VERSION:	
ORIGINAL VERSION:	
OWNER:	**GROUP CHIEF FINANCIAL OFFICER**
TYPE OF PAPER:	**POLICY STATEMENT**
TOPIC AREA:	**DATA PROTECTION**
DOCUMENT REF:	

A. PURPOSE

The purpose of this Policy Statement is to set out our responsibilities in relation to data protection, in order to protect the rights of individuals whose Personal Data is processed by ISP, Regional Offices and Schools within the Group.

This Policy Statement also provides information and guidance to those working for us on all aspects of data protection, including the retention and deletion of Personal Data, data sharing and how to handle subject access requests and/or any other requests for Personal Data.

B. SCOPE

This Policy Statement is **mandatory** for all Schools in the Group, and all parts of the business including ISP Central Office, and ISP Regional Offices.

The adoption date of this Policy Statement is 01/01/2019 and should be applied by all Schools and Regional Offices by 01/01/2019.

ISP Central Office, all Regional Offices and Schools determine the way in which the data they collect is processed and all have obligations as Data Controllers.

C. DEFINITIONS

Data Breach: an incident in which confidential and/or Personal Data is processed in error, and/or has potentially been viewed, stolen, or used by someone unauthorised to do so.

Data Controller: the organisation which determines the purposes and means of the processing of Personal Data.

Data Processor: a body (e.g. a third party) which processes Personal Data on behalf of the Data Controller.

Group: ISP and any subsidiary or related group company.

Incident(s): any threat or potential threat facing any aspect of the business, which (should it occur), would be likely to prevent or seriously hinder the day to day operations of all or part of the business.

Such threats include: natural disasters, site disasters (e.g. fire/flood/vandalism), epidemics, terrorist attack, off-site disasters, cyber-attack, death or serious injury of staff or pupils, safeguarding incidents where it is considered that pupils may be at risk of harm; violence to staff or pupils, hostage taking, strike action, bomb threat, infectious health hazard, arson, adverse media attention, any matter which might lead to criminal charges, and any matter which triggers a reporting requirement to a regulatory authority.

ISP: International Schools Partnership Limited.

ISP Board: The board of directors of ISP. This is the Group's strategic board.

ISP Central Office: The head office of ISP located in London, UK.

ISP Management Board (or "SMT"): The ISP senior management team.

Personal Data: any information relating to an identified or identifiable natural person (or otherwise defined in local legislation). Such data is 'processed' when it is obtained, recorded, held, disclosed/made available, retrieved, altered, or deleted/destroyed.

Policy Application Notes: Notes setting out the legal and regulatory requirements relevant to implementing the key principles of this Policy Statement, which must be fully up to date and compliant with the applicable laws and regulation/s relating to data protection in the relevant Region.

Region: United Arab Emirates, Latin America, USA and Europe, and such other region as the ISP Board may determine from time to time.

Regional Office: any ISP office in a Region.

School: Any school which is part of the ISP Group.

Sensitive or Critical Data: information classified in accordance with any legislative, regulatory contractual, or confidentiality requirements of each Region that is deemed to be of increased sensitivity or there are increased security requirements, as set out in the relevant Policy Application Notes.

Staff: any person employed or engaged by ISP, whether at ISP Central Office, at a School or a Regional Office.

Student: Any child or young adult enrolled on a course of study at a School in the Group.

D. ROLES AND RESPONSIBILTIES

The **ISP Board** has overall responsibility for ensuring that this Policy Statement complies with our legal and ethical obligations, and that those under ISP's control comply with it.

The Policy Owner has delegated responsibility for oversight of the implementation of this Policy Statement, and is responsible for:

- Appropriate reporting under this Policy Statement to the ISP Board, which shall be a minimum of once a year;
- Monitoring the effectiveness of this Policy Statement through regular review, and via an internal audit process. This will include an annual review of this Policy Statement;
- Putting in place a policy for ISP Central Office, and monitoring the effectiveness of that policy.
- Ensuring appropriate training for any relevant Staff at the ISP Central Office;
- Ensuring appropriate data sharing agreements are in place between ISP and Schools, and between ISP and the Regional Offices; and
- Ensuring that there are appropriate data processing and/or data sharing agreements in place between ISP and any other Data Controller or Data Processor.

The **ISP Management Board** is responsible for ensuring the implementation of this Policy across the Group and delegates day to day responsibility in each Region to the Regional Managing Directors, who in turn are responsible for:

- Developing Policy Application Notes, which are fully compliant with this Policy Statement and approved by the Policy Owner;
- Keeping the Policy Application Notes under regular review, and communicating any updates;

- Ensuring each Regional Office, and each School has its own Data Protection Policy, which is fully compliant with this Policy Statement and the Policy Application Notes;
- Monitoring the implementation and effectiveness of each Regional Office and School policy;
- Ensuring appropriate training is put in place for relevant Staff, appropriate to their role and in accordance with the Policy Application Notes;
- Ensuring that there is a designated, and appropriately trained, individual at each School with overall responsibility for data protection within the School; and
- Ensuring that there are appropriate data sharing agreements and/or data processing agreements in place between the Regional Offices and any Data Controller and/or Data Processor, including Schools within the Group.

All Staff in roles that may be impacted by data protection must ensure that they read, understand, and comply with this Policy Statement, and the relevant supporting Policy Application Notes and associated policies.

All Staff are required to avoid any activity that might lead to, or suggest, a breach of this Policy Statement. If anyone is unclear on any aspect relating to the application of this Policy Statement, they should seek guidance from the Regional Managing Directors for the Region or the Policy Owner.

Where there is a Data Breach, this must be reported as an Incident in accordance with the Crisis Management and Business Continuity Policy Statement.

E. KEY POLICY PRINCIPLES

ISP Central Office, all Regional Offices and Schools must have in place their own data protection policy which is compliant with this Policy Statement and incorporates the following principles, whether or not the local laws require it:

- The processing of Personal Data will be fair, lawful and transparent.
- The collection of Personal Data will be for specified, explicit and legitimate purposes.
- Personal Data processed by ISP shall be:
    - adequate, relevant and limited to what is necessary in relation to the purposes for which is it processed;
    - accurate, and where necessary, kept up to date;
    - kept in a form which permits identification of individuals for no longer than is necessary; and
    - processed in a manner that ensures appropriate security.
- A structured filing system for both electronic and paper records will be in place, and properly maintained.
- Any requirements to inform individuals (including Students, parents and Staff) how and why their Personal Data is being processed will be met.
- For Regions in which individuals have rights to request their Personal Data, appropriate procedures and training should be in place to ensure there is a process for responding to such requests.
- Particular care should be taken in relation to the sharing of Personal Data in relation to any safeguarding issues, to ensure that this is in accordance with the Safeguarding and Child Protection Policy Statement and any associated policy documents.
- Particular care shall be taken in relation to the management of (including the secure storage, appropriate retention, permission levels / access to and appropriate sharing) both Personal Data and Sensitive and Critical Data, to ensure that all relevant legal obligations are met.
- Procedures and technologies required to maintain the security of all Personal Data from the point of collection to the point of destruction will be in accordance with the IT and Cyber Security Policy Statement and any associated policy documents.
- Appropriate methods for the backup and storage of data should be in place and retention periods for Personal Data adhered to in accordance with the different obligations in different countries.
- Hard copy documents containing Sensitive or Critical Data should only be retained if absolutely necessary and should be kept securely. Such documents should be destroyed by means of confidential shredding.
- The way in which Personal Data is processed shall be subject to regular review.

- Schools will ensure that appropriate data sharing agreements and/or data processing agreements are put in place between the School and any Data Controller and/or Data Processor, including Regional Offices.
- USB sticks SHOULD NOT be used for Sensitive or Critical Data. Where any information is kept on a USB stick, this must be password protected and if lost or stolen, should be reported immediately to the Regional Managing Director as a Data Breach.
- Each Region should have their own policy in relation to the use of passwords for Sensitive or Critical Data which covers password requirements and how often passwords should be updated.
- The ISP website and those websites belonging to individual Schools should be carefully monitored in relation to the information that is published in the public domain and each website should display a privacy notice setting out the basis on which Personal Data will be processed.
- Procedures should be in place for the transfer of Personal Data outside of Europe and across countries.
- Regular training on data protection should be delivered to all Staff and those Staff in key roles should be updated on best practice.

F. CROSS REFERRED POLICIES

This Policy Statement should be read alongside the following:

- IT and Cyber Security Policy Statement;
- Crisis Management and Business Continuity Policy Statement; and
- Safeguarding and Child Protection Policy Statement.