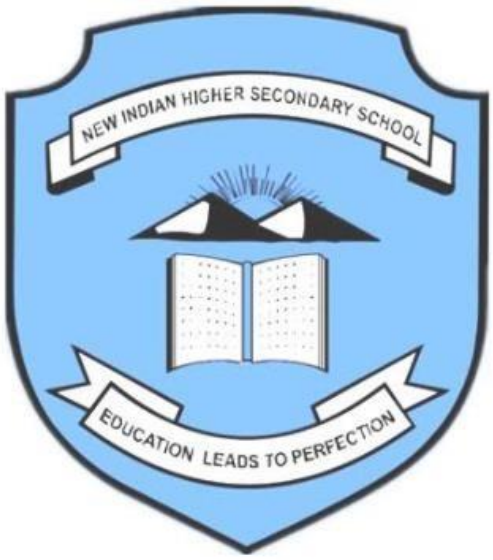
NEW INDIAN SCHOOL
RAS AL KHAIMAH



DATA PROTECTION POLICY

Agreed by:	Governing Body	
Review date:	4TH APRIL 2022	

NIS DATA PROTECTION POLICY

Introduction

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Data subject	The individual in relation to which the school is holding information about; in our context this is parents, pupils, staff, agency workers, governors and trustees.
Personal data	Information relating to identifiable individuals, such as parents, children, relatives, job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Personal data we gather may include: individuals' contact details, addresses, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV. Personal data may be collected from parents, staff, other schools, children, LAs, and the Department for Education.
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data is strictly controlled in accordance with this policy.

Scope

This policy applies to all staff, parents and children. Academy staff must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to staff use of internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

MRS BEENA RANI (PRINCIPAL)has overall responsibility for the day-to-day implementation of this policy.

The Data Protection Officer's responsibilities:

- Inform and advise the organisation and employees about duties and obligations to comply with data protection laws
- To monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed
- Keep the board updated about data protection responsibilities, risks and issues
- Review all data protection procedures and policies on a regular basis
- Arrange data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from parents/carers, staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by the NIS
- Ensure all IT systems, services, software and equipment meet acceptable security standards
- Ensure checking and scanning security hardware and software is carried out regularly to ensure it is functioning properly
- Researching third-party service providers, such as cloud services the company is considering using to store or process data

All staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UAE
- If there has been a data breach Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

Your data protection rights

- You have the right to ask us for copies of your information, which is free of charge in most cases.
- You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- You have the right to ask us to erase your information in certain circumstances.
- You have the right to object to the processing of your information in certain circumstances.
- You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.
- We may request proof of your identity before we disclose such information to you. That's so we can prevent unauthorised access. Just write to us at the contact details provided in the Contact Us section below.

GENERAL STATEMENT

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

• Inform individuals why the information is being collected when it is collected

• Inform individuals when their information is shared, and why and with whom it was 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

• Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests

• Ensure our staff are aware of and understand our policies and procedures

COLLECTING PERSONAL DATA

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

● The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before enteringinto a contract

● The data needs to be processed so that the Academy can comply with a legal obligation

● The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life

● The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest, and carry out its official functions

● The data needs to be processed for the legitimate interests of the Academy or a third party (provided the individual's rights and freedoms are not overridden)

● The individual (or their parent/carer when appropriate in the case of a student) has freelygiven clear consent

SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

● There is an issue with a student or parent/carer that puts the safety of our staff at risk

● We need to liaise with other agencies – we will seek consent as necessary before doing this

● Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:

o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

o Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share o Only share data that the supplier or contractor needs to carry out their service, andinformation necessary to keep them safe while working with us We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

● The prevention or detection of crime and/or fraud

● The apprehension or prosecution of offenders

● In connection with legal proceedings

● Where the disclosure is required to satisfy our safeguarding obligations

● Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents, or those with parental responsibility, which would like to see their child's educational record (which includes most information about a student) must make a request in writing.

CCTV

We use CCTV in various locations around the Academy site to ensure it remains safe. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Pr incipal.

PHOTOGRAPHS AND VIDEOS

As part of our Academy activities, we may take photographs and record images of individuals within NIS

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials upon enrollment to the School.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/ carers at the Academy for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos are not taken of other students unless express permission has been provided.

Uses may include:

● Within the Academy on notice boards and in the Academy prospectus, display photos around the Academy, and the newsletters.

● Outside of the Academy by external agencies such as the Academy photographer, newspapers, and campaigns.

● Online on our Academy website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.\ See our Safeguarding Policy, Social Media and Website policies for more information on our use of photographs and videos.

Data protection by design and default We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach.

TRAINING

All staff and the LAB are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Academy's processes make it necessary.

MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated on an annual basis to ensure changes are reflected appropriately

Complaints

Complaints will be dealt with in accordance with the school's complaints policy.

Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.