Privacy and Data Protection Statement

We are the Data Processor of the School that has instructed us. We are under no statutory obligation to share this information with you. To the extent that this information is insufficient or you have further questions please talk to the School.

1. Introduction

Privacy and security are at the heart of everything We do. This statement explains the key measures we have put in place to ensure that your data is kept secure and processed appropriately at all times. It covers our commitments to you, and what we expect in terms of privacy and data protection from Schools.

2. Our Principles

We:

Process the data received from Schools for the purposes of education and school improvement only, and only for those purposes necessary to provide the service explicitly offered to Schools.

Only store and process the minimum data required to provide our services, and to inform Schools in advance of using any of our services what data that service requires.

Transport and store all personal data originating from Schools using modern and best practice encryption technologies. This includes Secure Socket Layers (SSL/TLS) for encrypted data transfer over the internet, field-level encryption for personally identifiable data and password-protected identities for all end users.

Ensure that all data is held securely by taking steps so that data is not corrupted or lost.

Use encryption at rest i.e. when data is stored on a disk or laptop.

Use field level encryption in our database, where we feel it necessary to do so.

Ensure that all staff having access to personal data hold a valid Disclosure and Barring Service certificate or the equivalent in the Philippines.

May share anonymised extracts of writing for national projects for research and marketing purposes.

We DO NOT:

Share non-anonymised data with third parties, except where explicitly requested by you or required by law, or for the purpose of providing a service or where there is a legitimate interest to do this.

Transport personal data in an unencrypted format.

Claim ownership or exclusive rights over any of the data processed or created as part of services provided to you.

3. Security and Encryption

We have invested in security and we use a suite of modern encryption methods to secure the data held within NMM.

4. Staff access to data and security

Internal access to information is limited to only those who require it to perform their jobs. Other security safeguards include firewalls and physical building access controls. We use role-based identities and password protection on all platform services and apps.

All our staff are required to agree that they will abide by the Security and Data Protection Policy at all times and sign a Confidentiality and Non-Disclosure Agreement. All staff and contractors are required to undergo an enhanced Disclosure and Barring Service (DBS) check in the case of UK-based staff, or in the case of our Philippine-based Technical Support staff, the equivalent National Bureau of Investigation checks. No data is stored or transported outside of the UK or EU without using appropriate and secure technologies.

5. Privacy or Security Breaches

We as the processor shall assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (security, notification of data breaches to controller and supervisory authority, impact assessments and prior consultations) taking into account the nature of processing and the information available to the processor.

6. Communication

We will communicate with Schools but We will never communicate directly with you.

7. Cookies

A cookie is a string of information that a website stores on a visitor's computer. We use cookies for purposes such as helping us to identify and track visitors' usage and preferences. Schools can disable cookies in Schools browser, although this may mean that some features of our website do not work as they should.