No More Marking Ltd., 26 Bridgemere Drive, Framwellgate Moor, Durham DH1 5FG
Company Number: 08788417
www.nomoremarking.com

What is No More Marking?

Version 20250423

This document sets out our engagement. The document details how we process data and includes our terms and conditions including the exclusion of liability.

We provide a suite of secure, cloud-based suite of products to improve school assessment. The suite includes http://au.nomoremarking.com that allows schools to assess open-ended work by setting up tasks on paper, then scanning and uploading them before judges perform pair wise comparisons of the work. This assessment process is referred to as Comparative Judgement. The suite includes https://progression.nomoremarking.com/ which allows schools to assess multiple choice tests by setting up tasks on paper, then scanning and uploading them to be marked by Artificial Intelligence. The suite includes https://hub2.nomoremarking.com/ which is a depository of resources for schools to enhance their teaching of writing. The suite of resources together is known as "NMM."

We receive exam "scripts" which we check to see that the scripts can be easily marked using our methodology. The scripts are then made available for the school to judge.

We have staff in the Philippines who receive the scripts for checking. These staff are directly employed by No More Marking Ltd under standard UK employment contracts. The staff work using our systems and are subject to our rules and processes. This document provides further details of these arrangements.

We also assess oracy examinations (often referred to as Speaking and Listening). We regard recordings of people's voice as being "special category" data (i.e. sensitive data). Recordings can identify a data subject's ethnicity or other special category data.

We will have no contract or any other dealings direct with any School's students and will process their personal data on the strict understanding that the School has made the students aware of our involvement.

For the purposes of the GDPR we are the data processor and each school is the data controller for its students. This document satisfies Article 28 of GDPR. Although we are under no duty

to adhere to articles 13 – 19 GDPR we have made the following information available to students (https://www.nomoremarking.com/contact).

General Conditions

This Agreement details the licence we grant Schools to use NMM. By subscribing to and/or using NMM, any School is agreeing to the terms that appear below. We reserve the right to revise and update the General Conditions at any time effective on the date of posting to the Site the new and/or revised provisions.

Subscriptions
We offer a combination of free and paid-for services. In order to access National tasks and the writing hub, a School must have a valid subscription or trial. Before a School's subscription or trial expires, we will contact the School to let the School know of the expiration with a quote for the following period. If we do not hear back, we will issue a School a new invoice for the following period. Unless otherwise agreed in writing, paid-for services are non-refundable.

Unless expressly agreed with us in advance, each School must have their own separate subscription, and subscriptions cannot be shared by multiple Schools, whether within the same ownership, academy trust or federation or otherwise. If a School is found to be sharing its subscription with any other School without our prior permission, its account may be immediately terminated by us.

We reserve the right to temporarily suspend and/or cancel unpaid subscriptions.

Liability
Although we have no reason to believe that any information contained within NMM, including our Site, is inaccurate, we do not warrant the accuracy, adequacy or completeness of the information, nor do we undertake to keep the information updated. We do not accept responsibility for loss suffered as a result of School reliance on the accuracy or currency of information contained in the Site. We and our directors, officers, agents, employees and contractors do not guarantee or warrant that NMM will be uninterrupted, without delay, error-free, omission-free, or free of viruses. The content on NMM is provided "as is" without warranties of any kind, express or implied, including as to accuracy, timeliness and completeness. Neither we, nor our directors, officers, agents, employees or contractors will be liable for any loss or damage, howsoever arising (whether in contract, tort (including negligence), breach of statutory duty, or otherwise) in connection with Schools use of, and/or access to, NMM.

This exclusion of liability extends to loss of profits, sales, business, or revenue (direct or indirect); business interruption; loss of anticipated savings; corruption of data or information; loss of business opportunity, goodwill or reputation; or, any indirect or consequential loss or damage.

We are not excluding liability for death or personal injury caused by negligence, breach of any implied term and any other matter for which it would be unlawful to exclude liability.

Ownership of content
For all script images, Schools agree to give us the following permission: a non-exclusive, transferable, sub-licensable, royalty-free, worldwide licence to use any script images uploaded to any of our subscription-based products. We reserve the right to share anonymised images collected for any of our subscription-based products for research and marketing purposes.

Termination
We may suspend or restrict a particular School access to our services and NMM if we have reason to believe that the School may have breached the conditions of this agreement.

General

If a School does not comply with any part of this agreement, We reserve the right to suspend or terminate School access to our platform with immediate effect.

We and Schools both agree:

- That no failure or delay to exercise any right or remedy under this agreement or by law shall constitute a waiver of that right or any other right or remedy.

- That if any part of this agreement becomes invalid it will be modified to the minimum extent necessary to make it valid. If we cannot agree this with Schools, the relevant provision shall be deleted. Any modification to or deletion of a provision shall not affect the validity of the rest of the agreement.

- That any dispute or claim arising out of or relating to this agreement that cannot be resolved by negotiation within 14 days shall be resolved through arbitration. Either party shall give notice of seeking a resolution through arbitration using the CEDR procedure and English law. Either party may seek an interim remedy in court if necessary.

- That any dispute or claim arising out of or relating to this agreement shall be governed by the law of England and that the courts of England shall have exclusive jurisdiction provided that we can take action in other places if Schools are in breach of this agreement.

Data Protection with Schools

How do We comply with the GDPR?

As part of the compliance process, we have reviewed all our internal processes, procedures, data systems and documentation to ensure that we are compliant with the GDPR. We are happy to share our compliance regime. This is in addition to the requirements of Article 28.3(h).

Our GDPR Principles are:

- Data is processed fairly, lawfully and in a transparent manner;
- Data is processed only for specified and lawful purposes;
- Processed data is adequate, relevant and not excessive;
- Processed data is accurate and, where necessary, kept up to date;
- Data is not kept longer than necessary;
- Data is kept secure.

Data is not transferred to countries outside of the UK or the European Economic Area without adequate protection.

Sub-processors

We will only engage sub-processors with the prior general written authorisation of the School. If we intend to make any changes to our sub-processors under this general authorisation, we will inform the School in writing at least 30 days in advance of such changes, providing details of the new or replacement sub-processor and the processing they will undertake. The School shall have the right to object to such changes within 14 days of notification, providing reasonable grounds for objection related to data protection compliance. If the School objects and we cannot reasonably accommodate the objection or demonstrate compliance, the School may terminate the affected services.
We ensure that all third-party sub-processors we engage are bound by written agreements that impose the same data protection obligations as set out in this agreement, including sufficient guarantees to implement appropriate technical and organisational measures to meet GDPR requirements. We remain fully liable to the School for the performance of the sub-processor's obligations.

Assistance with Data Subject Rights

We will assist the School in responding to requests from data subjects exercising their rights under the GDPR (including rights of access, rectification, erasure, restriction of processing, data portability, objection, and automated decision-making) by implementing appropriate technical and organizational measures, insofar as this is possible.

Assistance with Controller Obligations
We will assist the School in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor.

End of Contract Data Handling

Upon termination of services, we will, at the choice of the School, delete or return all personal data to the School and delete all existing copies unless storage is required by law. Schools must notify us of their preference (deletion or return) upon termination of services.

Audits and Compliance Demonstration

We will make available to the School all information necessary to demonstrate compliance with the obligations set out in this agreement and will allow for and contribute to audits, including inspections, conducted by the School or another auditor mandated by the School, with reasonable notice.

International Data Transfers

We shall only transfer personal data outside of the UK and EU if we have implemented Appropriate Safeguards to ensure the protection of the Personal Data in the destination territory, in accordance with the applicable Data Protection Legislation.

GDPR Compliance Summary

We provide a summary below of important aspects of our compliance with GDPR for ease of use by schools.

Theme	**Details**
Subject matter of the processing	Assessment processing using our platform.
Duration of the policy	For the duration of the School subscription with Us.
Nature and purposes of the processing	Pupil information is collected, scanned responses to questions are uploaded to NMM with responses being judged. The pupil information collected (see "Contents" below) is used for association of assessment scores to pupils, and the analysis in terms of writing ages and by pupil group.
Source and type of data	The source of data is from the School and is information related to pupils in the School (see "Contents" below). The data is collected electronically and uploaded to our platform via a spreadsheet file.
Contents	Except oral transcripts, no special category data is collected. We only store and process the minimum data required to provide Our services. This includes personal level data for pupils. Information stored for pupils is:

	• UPN (optional) • First Name* • Last Name* • Date of Birth • Year Group • Gender • Group (teaching/registration class, optional) • Pupil Premium (optional) • Scanned Images of writing • Typed responses *Please note that names are collected to support the reporting to Schools. Information stored for teachers is: • Email address • Text comments • Audio comments
Processing and the role of the school	When a School decides to use Our system, the School will remain the Data Controller. We process the data on Schools behalf, in the manner Schools have requested. We only process data based on written instructions from schools except where required by law. Schools remain responsible for School data, including any inaccuracies or changes that need to be made. School responsibility as Data Controller covers all of School data on the platform.
Controlling access and use	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. We transfer data to our Philippines-based technical support staff using appropriate and secure technologies and processes (see “Security” below).

Data retention and destruction	We retain Schools' data on Our platform for as long as necessary to provide Our services. The connector will pull data from the moment Schools permission an application until the moment Schools delete it. This historical data is then held within the platform to allow Us to provide Schools with analysis over time. Deleting any task will delete all data and images associated with it. We will always notify Schools before We delete Schools data so Schools have the option to reactivate Schools account should Schools wish to. In addition to the above, Schools have the right to have all Schools data removed from our platform at any point in time. If Schools wish to do this then Schools should give us notice by emailing support@nomoremarking.com with the relevant details, and We will delete the data within 5 working days. We acknowledge that the oral recordings are more sensitive and we will delete within one year of receipt.
Security	We have invested in security and we use a suite of modern encryption methods to secure the data held within our platform. All external data transmissions to and from our platform are encrypted using modern SSL protocols and ciphers. Media files uploaded and products from these files are stored on AWS S3 storage (Ireland). The database is held on AWS servers (Ireland) and is provisioned using Mongodb Atlas. All data is backed up every night and on weekly and monthly rolling schedules. We use encryption at rest, i.e. when stored on a disk or laptop. We use field level encryption in our database, where we feel it necessary to do so. We use encrypted passwords with variable permissions according to the user's role are used for access to all sensitive information. We maintain no servers of our own as we are entirely cloud based. We believe that our cloud providers comply with the Data Protection Act 2018 and all ensuing laws or regulations including the General Data Protection Regulation (GDPR).

Breach	We take all reasonable and necessary precautions to ensure that School data is secure and to recognise and then mitigate the risks to security and privacy. However, it is not possible to 100% guarantee the security of any data transmitted or stored electronically. If a breach of security or privacy occurs, We will contact the Data Controller of the affected data, and if required inform the Information Commissioner's Office (ICO), and other authorities.
Automated Profiling	We do not carry out automated profiling.
Offshore storage	Media files are all stored on AWS S3 storage (Ireland). The database is held on AWS servers (Ireland). Both are backed up regularly by AWS.
Third parties	We will share information if required to do so by law. We will never rent or sell School data for marketing purposes. We will not share any sensitive or confidential information with third parties except in instances where We are specifically requested to do so by Schools. For example, some services on our Platform allow the sharing of School data with third parties such as school improvement charities and curriculum providers. In such circumstances, information is only shared if Schools give permission.

Third Party Websites

Crisp
Purpose: Crisp is our chat support hub for customers.
Data storage: All Crisp data is held on servers hosted in the 🇪🇺 European Union. Messaging data is stored in 🇳🇱 The Netherlands and Plugin data is stored in 🇩🇪 Germany. Servers are hosted by DigitalOcean (with a subsidiary in the EU subject to EU law).
GDPR statement: https://help.crisp.chat/en/article/whats-crisp-eu-gdpr-compliance-status-nhv54c/
We use third-party analytics services to help understand your usage of our services. In particular, we provide a limited amount of your information (sign-up date, coordinator name, phone number, job title & email address, purchased products, DfE number, school name and school address) to Crisp, and utilise Crisp to collect data for analytics purposes when you visit our website or use our product. As a data processor acting on our behalf, Crisp analyses your use of our website and/or product and tracks our relationship by way of cookies and similar technologies so that we can improve our service to you.

Crisp may store data in the form of cookies. For more information on their cookie policy please visit: https://help.crisp.chat/en/article/crisp-chatbox-cookie-and-ip-policy-1147xor/

We may also use Crisp as a medium for communications, either through email, or through messages within our product(s). As part of our service agreements, Crisp resolves end-user identity information (first and last name, avatar, company) from external APIs. Those external APIs source this data from public information that the end-user consented to share on a third-party service (eg. on social networks such as LinkedIn or Twitter). This end-user identity information is stored on Crisp services, for as long as the Crisp customer wishes them to be stored in their Crisp CRM database. The service used to discover such user information is Enrich, a service owned and operated by Crisp.

Brevo
Purpose: Brevo is our main customer email contact platform.
Data storage: *data is stored either on Google Cloud in Belgium or on AWS in Ireland.*
GPDR statement: https://www.brevo.com/gdpr/
The data stored on Brevo are: email addresses, names, dfe numbers and purchase history of account holders for paid subscription products only.

Amazon Web Services (AWS)
Purpose: AWS is used to host our website and deliver a serverless experience.
Data storage: These are our cloud hosts with the data centre located in Ireland.
GDPR statement: https://aws.amazon.com/compliance/gdpr-center.
Also for the UK Government's certification scheme Cyber Essentials Plus please see https://aws.amazon.com/compliance/cyber-essentials-plus.

MongoDB Atlas
Purpose: This is our main database storing all school, task & candidate information
Data storage: data is stored in Ireland as part of AWS.
GDPR statement: https://www.mongodb.com/collateral/gdpr-impact-to-your-data-management-landscape

Auth0
Purpose: user authentication on our website.
Data storage: Servers are located within the EU in Frankfurt.
GDPR statement: https://auth0.com/docs/compliance/gdpr
Auth0 is our authentication management platform enabling users to securely sign in and create accounts.

Anthropic

Purpose

- *Producing a summary of teachers' audio comments made while judging to produce reports for pupils.*
- *Transcribing anonymised images of writing so they can be assessed by an automated judging assistant.*
- *Automated judging.*

Privacy notice
https://www.anthropic.com/legal/privacy

How your data is used to improve model performance
We will not use your Inputs or Outputs to train our models, unless: (1) your conversations are flagged for Trust & Safety review (in which case we may use or analyze them to improve our ability to detect and enforce our Usage Policy, including training models for use by our Trust and Safety team, consistent with Anthropic's safety mission), or (2) you've explicitly reported the materials to us (for example via our feedback mechanisms), or (3) you've otherwise explicitly opted in to the use of your Inputs and Outputs for training purposes.

Data retention
The data is deleted on the backend within 30 days of receipt or generation.

Data transfer
The data may be transferred to the Anthropic servers in the United States but Anthropic ensures it benefits from an adequate level of data protection by relying on Adequacy decisions and Standard contractual clauses.

Data storage
Data is stored within the US.

Open AI

Purpose

- *Transcribing teacher's audio comments while judging.*
- *Transcribing anonymised images of writing so they can be assessed by an automated judging assistant.*
- *Automated judging.*

Privacy statement
https://openai.com/enterprise-privacy
How your data is used to improve model performance
https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance

Services for businesses, such as ChatGPT Team, ChatGPT Enterprise, and our API Platform
By default, we do not train on any inputs or outputs from our products for business users, including ChatGPT Team, ChatGPT Enterprise, and the API. We offer API customers a way to opt-in to share data with us, such as by providing feedback in the Playground, which we then use to improve our models. Unless they explicitly opt-in, organizations are opted out of data-sharing by default.

Data retention
OpenAI may securely retain API inputs and outputs for up to 30 days to provide the services and to identify abuse. After 30 days, API inputs and outputs are removed from our systems, unless we are legally required to retain them.

Data transfer
OpenAI encrypts all data at rest (AES-256) and in transit between our customers and us and between us and our service providers (TLS 1.2+), and uses strict access controls to limit who can access data.

Data residency
Data is stored within the US.

Data sharing permissions for analytics

In some limited circumstances We may collect non-personal and non-sensitive platform data through third party services. For example, we may use website analytics traffic providers to analyse metadata such as platform usage. Where We do this, We audit the service to ensure they have a similarly high level of commitment to security and privacy. These services may store Schools IP address, but we do not have access to this information ourselves. These services may store such data outside of the European Economic Area. We may also collect, analyse or make available non-sensitive data to third parties (for example aggregated or non-identifiable data) for School improvement purposes. We do not use or analyse this aggregated data in any way which would make data identifiable at an individual or School level.