Dyslexia Gold DPIA

Submitting controller details

Name of Processor	Dyslexia Gold
Subject/title of DPO	Data Protection Impact Assessment
Name of DPO	Shane Williams (Global Policing)

Need for a DPIA

Dyslexia Gold is a complete programme designed to improve the teaching of those with dyslexia.

In order to deliver this programme, Dyslexia Gold collects data on users of the platform. The data processing involves analysis assessments of their users, as well as administration of website access, communication and invoicing.

The DPIA has been put in place due to access possible high-risk processing below and to be able to evaluate the risk and reduce any risks to an acceptable level.

1. Children's data being included in the Application
2. Identification or assumption that users are dyslexic

The DPIA has also been developed to allow a full overview of this project, allowing a greater understanding of how all parties data is used and any associated risks involved.

The Process

Data collection: Data is collected from teachers and other staff entering data onto the website. This is a combination of direct, manual data entry into the main Dyslexia Gold Wordpress website or embedded Google Forms, and the upload of pupil data in a CSV file directly into the analysis website

Storage: All data is stored on a secure server.

Data use: Staff data is used to administer access to the website and communicate with staff involved in Dyslexia Gold, as well as ensure that staff have a good understanding of the teaching. Pupil data is used to help assess children and analyse progress and gaps in understanding for individuals and groups of pupils.

Data access: Only Dyslexia Gold staff have access to the data held by them.

Data sharing: Data is only shared between the client and Dyslexia Gold. Dyslexia Gold does not directly share data with third parties.

Data sub-processors: There is no Sub Processing.

Retention periods: Data will normally be retained for as long as a client has an account and for 1 after the end of the licence period, or when a client requests that their account and all associated pupil data is deleted. Teacher and pupil data can also be manually deleted by schools.

Security measures: Best practice security measures are used to protect personal data, including security certificates on websites, use of encrypted laptops for any data held locally, and strong password standards. All staff at Dyslexia Gold involved in the processing of pupil data are DBS checked and sign an information security policy. They also do data protection training as part of their induction and refreshers as policies are updated.

New technologies and novel types of processing: All processing activity uses standard, off-the-shelf products and functions (e.g. Excel and Google Forms) plus a

system designed specifically for pupil analysis using processing steps which have previously been used in multiple tracking systems.

SCOPE OF PROCESSING

Type of data and sensitivity: The personal data on staff includes name, organisation, role and contact details. The personal data on children includes name, unique pupil number and demographic characteristics (date of birth, ethnicity, gender, year group, special educational need provision, first language,), so is sensitive data including protected characteristics.

There will be an assumption that users of this platform have dyslexia**.**

Some financial information is held on the server in particular the organisation subscription contacts and invoice details. No bank details are held.

Frequency and duration: The processing of staff data will largely be a one-off exercise at the start of the period when the school signs up to Dyslexia Gold. There will likely be additional processing of staff data each year when new staff join a organisation and undertake training. Organisations may also update staff details through the year or remove access when a member of staff leaves.

Processing of pupil data will happen at the start of each academic year (when pupils are uploaded into the analysis system), when new pupils arrive, and when assessments are carried out (normally 6 times per year at the end of each half term).

Data sources: Staff data is provided by clients when signing up for Dyslexia Gold and setting up other staff on the website. Staff assessment data is added by the staff themselves. Pupil details are added either by the client or themselves.

Relationship with individuals whose data is processed: All staff and pupils belong to a client organisation that has signed up to Dyslexia Gold. Clients in particularly schools, have a statutory duty to provide high-quality education for their pupils and, in particular, support pupils that need additional targeted interventions. The processing of data for Dyslexia Gold enables them to do this.

THE PROCESS

The processing of staff and pupil data will enable organisations to fulfil their statutory duty to offer high-quality support and education to clients with dyslexia.

Staff data will be processed to allow organisations to be set up on the Dyslexia Gold and access training, support materials and other content on the website. It will also be used to enable staff to carry out their CPD assessment which will be used to provide the manager with information on the ability and understanding of their staff. This means that staff who need additional training or support can be identified, so that high-quality phonics teaching can be rolled out across the school.

Pupil assessment data will be processed to help organsations analyse the progress of their pupils and understand where individuals or groups of pupils need additional support, and what their next steps for development are. This may include analysis of groups of pupils (e.g. by ethnic group) which means that schools can provide targeted support and meet their Public Sector Equality Duty to advance equality of opportunity (https://www.gov.uk/government/publications/public-sector-equality-duty).

Consultation process

Global Policing was consulted to look over the DPIA and advise.

Assess necessity and proportionality

Lawful basis for the processing: Legitimate Interests for the parties using the applications.

Preventing function creep: Given the focus of the application, the only new developments on the use of data will relate to enabling organisations to better support their pupils and train their staff in dyslexia provision. New developments will therefore largely be in response to requests from organisations on how to better support them to improve the dyslexia support.

Quality: Data quality will be maximised where possible by pre-populating information already held in data entry forms. For example, user details and organisation IDs are pre- populated in the staff assessment form from the original records that have been created and checked when setting up the organisation. Pupil details should, where possible, be uploaded from data held on a organisations own MIS to avoid re-entry of data and risk of error.

Data minimisation: Only pupils for whom dyslexia support is needed will be included in the pupil data.

Note that most staff in a organisation are encouraged to complete the CPD training so that there can be a consistent, whole-school approach.

Provision of information: Organisations will be able to request all assessment data held on their own staff and pupils. This will be by downloading from a website or by secure email. The privacy policy will be available on the Dyslexia Gold website.

Individual rights: If parents or pupils wish to see the assessment data that is held on them on the Dyslexia Gold system, they should contact the school who could extract pupil level data from the system to share. However they can contact our data protection service, who will be more than happy to assist.

Processor compliance: We ensure our data processors comply with security policies through their own privacy policy and information security training. Although we do not require one, we also have an independent data protection service, Global Policing.

Possible Risks

Potential Impact on individuals.	Likelihood of harm	Severity of harm	Overall risk
Inability to exercise rights (including but not limited to privacy rights)	Possible	Significant	Medium
Inability to access services or opportunities	Possible	Minimal	Low
Loss of control over the use of personal data	Possible	Significant	Medium
Discrimination	Remote	Minimal	Low
Identity theft or fraud	Possible	Minimal	Low
Financial loss	Remote	Minimal	Low
Reputational damage	Possible	Significant	Medium
Physical harm	Remote	Minimal	Low
Loss of confidentiality	Remote	Minimal	Low
Re-identification of pseudonymised data	Remote	Minimal	Low
Any other significant economic or social disadvantage	Remote	Minimal	Low