

helloData Privacy Notice

Introduction

On the 25th May 2018 the new and updated General Data Protection Regulation (GDPR) came into effect.

This means that organisations and educational establishments need to be more careful about the way information and data is managed.

The DPA law (1998) was developed to protect individuals against misuse or abuse of information about them and preventing the sharing of data without consent.

The GDPR are designed to ensure the safety and security of all data held within an organisation (including schools, academies and other educational establishments). It's focused on looking after the privacy and rights of the individual, and more focused on transparency in terms of what data is held about individual's and how it will be shared and used.

The GDPR includes the requirement for organisations to review the technical and organisational measures in place to protect against unlawful processing, accidental loss or destruction.

How does GDPR affect schools?

The GDPR will change the way that educational establishments handle their data and the way information is managed. Any failure to comply with the regulations could result in fines and damage to reputation.

Our GDPR Principles are:

- Data is processed fairly and lawfully
- 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 processed in accordance with an individual's consent and rights

- Data is kept secure
- Data is not transferred to countries outside of the European Economic Area ('EEA') without adequate protection

How does GDPR affect sharing data with helloData?

You will need to ensure, when you share data with us for the purposes of providing the assessment reports and associated support (as per the contract that your school should have with us), that we are adhering correctly to the requirements of the law and in accordance with your own policies.

The purpose of this document is to explain what we will be doing in terms of ensuring GDPR compliance.

The lawful basis for sharing data with helloData & Suppliers

helloData acts as a Data Processor for attainment and progress data supplied by the schools. Each school acts as the Data Controller for this data.

If we need to access or see school data to be able to offer support to the school, then this will be lawful due to the requirement to fulfil a contractual agreement that we should have in place with the school.

helloData access to data

Any person involved in the support or processing of this product will have access to the data provided to helloData by the schools. As outlined above, if we need to access or see this data in order to offer support then this will not require further permission. We will obtain permission before dialling in to your MIS system if this is required to further investigate problems reported by you.

helloData grants access for the purposes of providing support and processing to Turn It On Ltd (MIS staff) and Marczak Assessment Solutions, thereafter known as the 'Suppliers'. All Suppliers will adhere to this privacy notice and helloData's Terms and Conditions.

helloData also grants access to any, previously agreed, at the time of purchasing the product, third partner support partners, for example local support units and RM, for the purpose of providing support only, thereafter known as the 'Support Partners'. Support Partners are bound by our Terms and Conditions. Schools should refer to the Support Partners' Privacy notice.

Training

All of the Suppliers have undertaken GDPR training.

On-site work

The Suppliers have clear guidelines with regards to keeping data secure – this includes always seeking permission from the school before accessing data on site, accessing data in an agreed secure manner and not disclosing user logins when provided by the school for the purpose of support.

Remote Access and On-site Access

The Suppliers involved in providing direct support to the school can enter the school's data either remotely via Autotask, on site at the school using Team Viewer which involves the school entering an access code, or through a unique login provided by the school. All helloData Suppliers have an admin login for each school account on the helloData website (reporting tool only). The login information is kept secure at all times and is only used for the purpose of support.

All Suppliers will follow the appropriate access control procedures.

Data that we may hold for your school

Contact information

The Suppliers hold information on registered users including school name, DfE number, user name, email address and position in school, where relevant. This data is provided by the school and consented to by the headteacher. This information is collected and stored for the purpose of account verification and for the duration of the contract.

Data Items

The Suppliers hold data, provided by the school either through the use of management Information System API or by manually uploading the data, for the purposes of producing the reports and providing support only.

Pupil data items include: UPN, Date of Admission, Date of Leaving, Pupil forename, surname, gender, registration, year group, date of birth, percentage attendance, SEN status, EAL, Ethnicity, looked after status and eligibility for pupil premium, free school meals, ever6 free school meals and service indicator.

Membership of student groups/user defined groups is also used.

Assessment data items include: EYFS attainment, KS1 attainment, Nursery to Y6 attainment and progress figures, where relevant to the type of school.

The data items collected are reviewed and updated at regular intervals, the school will receive notification when data items change and are in control as to when and if the data is included. This policy will be updated when data changes.

Data held is stored securely

Your data is uploaded into an SQL Server database hosted in Microsoft Azure's UK South data centre. It is backed up daily in the same data centre. The website is only accessible over https (secure connection) so all login and school data is encrypted in transit. Once your data is processed it is placed into the reporting dashboard which uses Microsoft's app.powerbi.com service, again hosted in the UK South data centre.

Password and credentials information

Where provision is made, it is the school's responsibility to grant permission to helloData to access the data through the management information system API. In this instance the school is in control as to which data fields are taken. Where the API is not available, it is the school's responsibility to upload data belonging to the school onto the helloData website. Where support is required, permission from the school to access the data and/or school systems will be sought.

By completing and signing the helloData order form, the headteacher is granting permission for the Suppliers to create one admin user account on the helloData platform. It is the responsibility of this user to create and manage user accounts for all other users within their school. If the school is using RM Unify to access helloData, the user accounts will automatically be generated. The Supplier will grant helloData admin access to the RM Unify admin user of the school. This user will be responsible for managing the permissions of other users within the school.

The Suppliers do not have access to, or store unencrypted user passwords.

It is the school's responsibility to delete accounts of users that are no longer required. The Suppliers will remove access to a user upon request. In the event that the school no longer requires the data to be processed, the school must notify the Suppliers as soon as possible and all data will be deleted.

Inherited policies on consent etc.

We will not be accessing, viewing or using your data in any way other than to assist with your problems. Therefore, all issues of consent, individual rights, appropriateness of data etc., will be inherited from you, the school.

How we handle your data

Suppliers will ensure that information is not kept longer than is necessary and will retain the minimum amount of information that it requires to carry out its' contractual functions and the provision of services.

We make our systems secure and keep any paper files with customer information etc. locked away securely.

End of life

If we need to print anything from your data for the purposes of resolving your issues, or if you email us any documents that we need to print, these will be shredded once the issue has been resolved.

We will not copy your data onto CD or DVD but if we receive any of these with data on, they will be shredded after resolution. Data sticks received from the school will be wiped and returned or destroyed. We will not request data is sent to the Suppliers via email but, in the event that the school chooses to do so, all emails are secure and we will not forward data on to any other 3rd parties other than the aforementioned Suppliers.

Our Suppliers and Support Partners

We expect our Suppliers (Data Processors) and Support Partners to have the correct GDPR processes and procedures in place.