Privacy Notice - Schools Data and turn IT on

Introduction

On the 25th May 2018 the new and updated General Data Protection Regulation (GDPR) will start to be enforced.

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

Version: 1.1 Release date: July 2022 Review date: July 2023
Authorised by: Head of Data Protection/HR & Finance Director

- 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 turn IT on?

You will need to ensure that if you need to share data with us for the purposes of 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.

Turn IT on access to data

Many of our staff will have access to the data held by our schools – either on site or remotely.

This could be employees in roles such as an on-site ICT consultant or an off-site MIS consultant or a Helpdesk role.

Anyone that has access to schools or to the systems that we use to access schools' information has already gone through very thorough safeguarding checks – more information can be found in our Safer Recruitment Policy and our Safeguarding and Child Protection Policy.

Training

All staff are given basic GDPR training upon induction and with annual updates.

Managerial staff and staff with access to restricted systems have more intensive GDPR training.

All staff that work in schools or have access to schools' date have Safeguarding training.

Staff have clear guidelines with regards to keeping data secure – this includes the Protecting Schools Data Policy that we issue to employees upon induction and that we ask staff to confirm receipt and understanding of.

Cyber Essentials

Achieving the Cyber Essentials certification was seen as a way to demonstrate a level of assurance to our customers, by showing that security controls are in place to protect the business, its IT systems and information, and that these controls have been assessed against an independent, formal framework.

Version: 1.1 Release date: July 2022 Review date: July 2023
Authorised by: Head of Data Protection/HR & Finance Director

On-site work

Staff that work on-site at schools are required to adhere to the guidelines with regards to keeping data secure. Staff will have had the relevant safeguarding checks and training with regards to safeguarding and data protection.

Remote Access and On-site Access

Relevant staff can enter schools' systems either remotely via Autotask from TIO offices or on site at the school.

We have an Access Control Procedure for staff to follow which we monitor and update on a regular basis and communicate with staff.

Leavers

Within 24 hours of someone leaving the business the Helpdesk team terminates access to office 365, Autotask and other systems. HR terminates the employee on the HRM system and closes access to the staff portal, school's portal and credentials manager.

Data that we may hold for your school

Contact and payment information

Turn IT on hold data about schools in terms of our customers including the school name, address, phone and email and a record of items that you have purchased from us and with regards to invoices, payments etc. We do not accept card payments – only bank transfers and cheque payments – so have no record of any card or bank details.

We hold data such as a contact name for each school, a contact email that you have supplied to us and sometimes a direct phone number.

Data held is stored securely in a CRM or in our staff portal system that is password protected and only accessible via a secure website which uses HTTPS and SSL to provide end to end encryption.

Password and credentials information

The Credentials Manager is a tool developed to store all Credentials information that we have for our schools. This could be any credentials from Windows Logins, Licencing account details and online services. The data is encrypted and stored in a way that is auditable and will allow us to tell a school exactly what credentials we store for them.

To access the Credentials Manager staff will need access to the staff portal (only existing staff will have this) and the member of staff will need to know the password. This password will be reset at least 3 times per year but could change at any points subject to unforeseen circumstances.

Support tickets

Schools have control over who can be a user and who can be a super user. Users can only see their own tickets; super users are able to see all tickets. This means that the schools can decide on who needs to see the information on all the support tickets and ensure that data is not being shared unnecessarily.

Information for MIS support

Commented [DS1]: We may also need to list MIS providers as sub processors? We will send information to them for more advanced support calls.

Commented [SB2R1]: The schools have separate contracts with the MIS providers such as Capita and so they should have one with us and one with Capita but we shouldn't need one with Capita I believe..

Our staff will be able to access systems with details that are provided by schools.

Schools have direct contracts and agreements with the software suppliers themselves.

In most cases turn IT on will not need to download any data. On a rare occasion that this should this be required the employee will be expected to ensure the security and safe disposal of the data.

The lawful basis for sharing data with turn IT on

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. We expect that schools (the Data Controller) will have their own data processing agreements that they provide to us (the Data Processor).

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.

turn IT on
Connecting schools and technology

How we handle your data

The data that we store on our systems relates to school contacts, tickets, service updates, bank information and the information required to fulfil our contract with you.

Turn IT on 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. Data used to resolve support calls will be kept for 30 days after the support call has been closed. Support tickets are kept for the duration of a support contract to help plan and manage support requirements and potential fault patterns.

We make our systems secure and keep any paper files with contract 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 schools will be wiped and returned or destroyed.

Our own redundant or broken computers have their hard disks removed before disposal.

Our partners

We expect our partners (Data Processors) to have the correct GDPR processes and procedures in place and ask our partners to sign our Data Processing Agreement to this end.

Data Protection Officer

Martin Long

Head of Data Protection

Email: DPO@turniton.co.uk

This privacy notice may change from time to time in line with legislation or industry developments. We will not explicitly inform our clients of these changes. Instead, we recommend that you check this page occasionally for any policy changes.

Version: 1.1 Release date: July 2022 Review date: July 2023
Authorised by: Head of Data Protection/HR & Finance Director