Target Tracker – EYFS and Primary Student Data Policy Statement

Introduction

Within Target Tracker, each school account contains information that allows the school to track the progress of their children and allow us to provide appropriate comparative and benchmarking data to create meaningful reports relating to progress and attainment. Details of specific schools or students are never released without permission of the Headteacher, Target Tracker aggregates data for statistical analysis and research, which may be published and used to provide comparative data to other schools and bodies interested in education.

The information we hold is held very securely and we take seriously our role in storing and processing that data on your behalf. We have a separate policy for data supplied by individuals in our Privacy Statement.

What Student Data is used?

We store the following data for each student:

UPN (Unique Pupil Number), Surname, Forename, Date of birth, Year Group, Date of Entry, Gender, FSM (Free School Meals), Pupil Premium, Ethnicity, First Language, EAL (English as an Additional Language), SEN (N- No special educational need A- School or Early Years Action P- School Action Plus S- Statement of SEN E- Education and Health Plan K- SEN Support), Gifted, Talented, In Care, Class, Preschool Exp (Number of terms before Reception), Previous Setting, Age, Terms Completed (Number of terms in setting), Attendance data, Transfer School data, school entered pupil notes, Postcode.

We store assessment data relating to teacher assessments, tests and progress through Assessing Pupil Progress and schools may choose to store textual comments and photographic "Observations".

Children's data supplied by schools does not contain email or postal addresses other than the postcode.

Who controls Student Data?

Initially, Student Data can be exported from SIMS or other school management software. Data is then added by the school or by us on your behalf.

Schools control their own Student Data, and can add, modify and delete student data without our involvement.

We only store your Student Data while there is a formal agreement between us. We will delete data from schools within a year of them ending their subscription with us. This is in case they change their minds and decide to re-subscribe or because they need us to work with their data so that it can be used in another system.

Security

We store Student Data on a secure server using encryption and firewalls to protect the information from being accessed by anyone else. Periodically, an external company carry out a penetration test to ensure all systems are as flawless as possible.

Your school has an encrypted security key so that only those with your key can access the school data. In addition school staff are assigned passwords that protect access to the system and ensure that only staff or those you choose to give permission to, such as advisers can access your Data. No 3rd party can access it without permission. Target Tracker does not keep your passwords, should you lose your admin password, we can simply re-issue you with a new

one on receipt of a request from the official school email. Further details of our security arrangements are shown below in appendix 1.

Data Protection Act

If you are unsure, guidance for schools on data protection policy can be found on the data protection website http://ico.org.uk/for_organisations/sector_guides/education

Essex County Council's data protection notification number is Z6034810

The Data Protection officer is David Wilde, Chief Information Officer for Essex County Council.

Usage by staff of the system.

Staff with administrator rights can view all logins to the system by all their staff. To ask for particular details, please phone our Help Desk on 01245 213141

Appendix 1

Target Tracker – EYFS and Primary Security

This document details the security arrangements within Target Tracker – EYFS and Primary.

We take security very seriously. Target Tracker employs methods equal to or better than other similar systems you may be used to. The following details outline the major points starting with the basics and then in more technical detail.

The Basics…

Software, not web page

Target Tracker requires the software to be installed to use it. The data cannot be accessed without it.

Encrypted login key, and user passwords

Simply installing the software is not enough. A 550 character encrypted login key, consisting of seemingly random letters, numbers and symbols, is provided to each subscribing school. It is impossible to access the schools data without it.

Every user within a school, additionally, has their own username and password that may be as complex as desired and changed as often as a school requires.

Encrypted data

When Target Tracker accesses the school data it uses an encryption protocol called SSL which is the same as that used in online banking. This ensures that nobody can intercept and read the data.

Cloud based storage from Microsoft

To ensure that we provide the best, most secure service to you we have chosen to use Microsoft's Azure Cloud storage system. Using a service provided by an international company like Microsoft means you can rest assured that the latest, most effective technologies are being applied.

A bit more technical detail…

Transport

All communications between Primary Target Tracker and SQL Azure are encrypted (SSL) at all times. No data is sent/received as plain text.

The SQL Azure server certificate is validated upon connection to prevent 'man in the middle' attacks.

Access

Authentication with Azure is performed using SQL Credentials which are stored encrypted on the server, and never transmitted over the wire unencrypted.

The SQL Azure environment employs FIPS 140-2 encryption

- In a TLS handshake, the client sends a list of ciphersuites that it supports and has enabled, and the server selects one from the client's list that it also supports and has enabled. As such, one of the following two outcomes will be produced:

1) There is a ciphersuite in the client hello message that is allowed by the FIPS 140-2 configuration on the server, and a connection is negotiated with a FIPS 140-2 ciphersuite.

2) There is not a ciphersuite in the client hello message that is allowed by the FIPS 140-2 configuration on the server. The server closes the connection with an "algorithm mismatch" error, and the client is unable to connect

Access to the school data requires a 550 character login key provided by Target Tracker, additionally the school must configure individual users protected by passwords. The access level of these users can be set to read-only-nonames/read-only/limited read-write/read-write/admin.

Login keys can be revoked, preventing any access to that school data. Requiring a new login key to be generated and provided to the school.

Storage

Data is stored in Microsoft's European Data Centre located in Dublin, Ireland

Microsoft Cloud

Microsoft's cloud infrastructure, including SQL Azure, is committed to annual certification against the ISO/IEC 27001:2005, a broad international information security standard.

The ISO/IEC 27001:2005 certificate validates that Microsoft has implemented the internationally recognized information security controls defined in this standard, including guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

Microsoft Azure also has Impact Level 2 (IL2) PROTECT and cesg G-Cloud accreditation.

More detail http://azure.microsoft.com/en-us/support/trust-center/compliance

Port TCP1433

Target Tracker requires outgoing access to TCP Port 1433. As an outgoing only, not incoming, connection any security risk is greatly reduced.