# Description of Security Measures Employed to Safeguard the Processing of Personal Data (Target Tracker)

## 1. Organisational

### a. Policies and Documented Procedures

EES for Schools (EES) and Target Tracker are compliant with the General Data Protection Regulation (GDPR). We give this assurance ahead of GDPR enforcement in May 2018. To ensure compliance we have been working with the Essex County Council (ECC) Information Governance team to put all requirements in place including those given as examples as they apply to our service.

Essex County Council has in place an effective framework to oversee compliance with GDPR (& supporting UK laws) with support from the Data Protection Officer. The Council has robust measures in place for ensuring that information is managed in a safe and secure environment. Our information governance framework establishes and quality-assures our information management framework. Our information governance framework clearly sets out the authority and relationships of relevant groups and roles. We have in place an effective process for managing complaints about how we handle information.

Our policies, strategies and standards are reviewed annually and whenever legislation changes to ensure they continue to deliver legislative and regulatory compliance and meet business needs. Our procedures and operational guidance are reviewed whenever relevant policies, strategies or standards are revised and when an operational need arises. Our project and technology governance mechanisms include appropriate checkpoints to ensure compliance with our information management framework, including the implementation of privacy impact assessments when information about people is involved.

As part of ECC, EES operates within strict and robust security measures compatible with, but not certified to, ISO/IEC 27001 standards. Target Tracker uses Microsoft Azure cloud for all school assessment data. As an enterprise and local authority customer of Microsoft, we ensure those systems are compliant and hold certification. Microsoft Azure ISO27001:2013 certificate number IS 577753.

### b. Roles

Essex County Council, ICO Registration Number: Z6034810

Data Protection Officer: Paul Turner

The Information Governance Team is the core function for managing information governance across the council and with our partners. Ensuring processes are robust and security breaches are dealt with and escalated appropriately in line with the Information Risk Escalation Process.

First point of contact, EES for Schools Software Operations:
David Neal (david.neal@EESforschools.org)

### c. Training

Access to information is limited to those staff with essential need only.

Those staff are subject to the standard safer recruitment procedures in place through ECC, including background checks, and undergo training as applicable to ensure the smooth running of the service.

Training and awareness in information governance is carried out according to a published training plan with all employees completing training within six weeks of starting employment and refreshing and updating that training every two years.

All EES employees are required to conform with ECC's information policies including corporate governance, data protection and privacy, using IT tools securely and acceptable use of resources including IT resources.

### d. Risk Management & Privacy by Design

As part of ECC, EES and Target Tracker adhere to the ECC Risk Management strategy which may be reviewed online at https://www.essex.gov.uk/Your-Council/Strategies-Policies/Code-of-Governance/Documents/RM_Strategy.pdf

This document details change management in detail including that the risk management policy & strategy, guidance and associated tools are regularly reviewed to ensure the impact of new legislation, government guidance or internal changes in practice are captured and reflected.

In addition to this, the Microsoft Azure services are regularly internally reviewed to ensure they meet requirements.

Application development follows an agile software development approach in which software security is a quality metric.

Security is considered from the initial point of specification gathering and continually challenged through the development phases. It is extensively and meticulously tracked in an issue management system using the industry standard which is cross-referenced with the code via an industry leading version control system.

Detailed issues are tracked using a combination of issue tracking collaborated with a version control system. Testing includes security and developers design and code using certified ethical hacker principles. Continuous integration allows each check-in to be verified by an automated build, ensuring early detection of any problems.

### e. Contractual Controls

Target Tracker data is hosted on the Microsoft Azure cloud.

Microsoft are fully compliant with security management standards as detailed earlier.

Further records, certificates and current information and policies therein may be found on the Microsoft Compliance web pages at https://servicetrust.microsoft.com/Documents/ComplianceReports

Target Tracker's customer database is hosted by a third party, Avrion (www.avrion.co.uk); a non-disclosure agreement is in place.

### f. Physical Security

School Assessment Data is stored in Microsoft's European Data Centre located in Dublin, Ireland and a backup is maintained in Chelmsford, England.

Windows Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24 hours a day, 7 days a week and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These data centres comply with industry standards for physical security and reliability and they are managed, monitored, and administered by Microsoft operations personnel.

Microsoft uses industry standard access mechanisms to protect Windows Azure's physical infrastructure and datacentre facilities. Access is limited to a very small number of operations personnel, who must regularly change their administrative access credentials. Data centre access, and the authority to approve datacentre access, is controlled by Microsoft operations personnel in alignment with local datacentre security practices.

If a school's data is submitted to us for processing, it is processed within our premises in Chelmsford, England and stored on ECC's own secure servers.

Visitors to council offices report to a central reception area. Employees carry identification badges and entrance to offices is controlled by swipe card. Access to our buildings is swipe access card controlled using the photographic ID card. All visitors have to be accompanied by a member of staff at all times.

The council's site is alarmed and has 24-hour CCTV surveillance. The site, including car parks, is security patrolled by the council's partner, MITIE (https://www.mitie.com/landing/). EES offices are on the first floor and not visible from the outside. Windows are lockable and have blinds.

### g. Security Incident Management

All information security incidents are reported to ECC's Information Governance team who will assume responsibility for investigating and resolving the issue. Each incident will be investigated to determine its impact on confidentiality, integrity and availability. Where customers' personal data is at risk, affected and potentially affected customers will be contacted without undue delay and in accordance with the GDPR.

## 2. Technical

### a. Data at Rest

i. Use of Hosting Services

School Assessment Data is stored in Microsoft's European Data Centre located in Dublin. No data is transferred outside the EEA.

Azure SQL is a multi-tenant environment. There is no access to the physical SQL Azure servers. There is no ability to access the physical servers hosting the databases as SQL Azure is a Platform as Service model. There is therefore no mechanism for one tenant to access any underlying data such as the database or log files from a multi-tenanted database. This removes a whole category of potential risks around management of multi-tenanted data.

All access to the database is channelled through SQL Azure Logical Server (Gateway). There is therefore never any direct connection from the client to the SQL Server instance. The Gateway ensures the separation of the two tenants sharing an underlying SQL Server database server. This logical layer is providing the logical separation of two tenants and ensures that the authenticated client can only access their data and ensures the scope of the connections. In SQL Azure you cannot issue commands such as Use Database to switch databases, a new connection to the Gateway must be established. As all the SQL TDS commands pass through the Gateway, Microsoft has been able to ensure the security boundary and can inspect all TSQL commands executed and enforce the multi-tenant security isolation boundary.

The customer relationship management (CRM) database for Target Tracker is hosted in the UK, within a Tier 4 datacentre. The CRM solution utilises a private virtual server dedicated for Target Tracker, and within our own server racks using our own infrastructure.

Access to the CRM system is completed via browser with unique username and password. Data in transit is secured using 256 bit encryption SSL for the entire site. Access to the server is via RDP, secured by unique username and password.

The CRM database uses MS SQL Standard Edition. The ‘Always Encrypted’ feature available in SQL2016 has not been used but is subject to review.

ii. Vulnerability Management

Microsoft Online Services implements technologies to not only monitor the platform for vulnerabilities but also to proactively identify vulnerabilities. Identified vulnerabilities are monitored, tracked, and verified by a security team which also ensures remediation. In addition, the Risk Management Team performs formal regular vulnerability assessments to identify vulnerabilities and determine whether key logical controls are operating effectively. These findings are categorised based upon risk, and updates to the environment are performed accordingly.

Microsoft Online Services subscribes to Microsoft’s Security Response Service and regularly monitors external security vulnerability awareness sites. As part of the routine vulnerability management process, Microsoft Online Services evaluates our exposure to these vulnerabilities and leads action across Microsoft Online Services to mitigate risks if necessary.

Microsoft Azure SQL Threat Detection provides a new layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. Users receive an alert upon suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns. SQL Threat Detection alerts provide details of suspicious activity and recommend action on how to investigate and mitigate the threat. Users can explore the suspicious events using SQL Database Auditing to determine if they result from an attempt to access, breach, or exploit data in the database. Threat Detection makes it simple to address potential threats to the database without the need to be a security expert or manage advanced security monitoring systems.

Microsoft Online services run multiple layers of anti-virus software to ensure protection from common malicious software.

Servers within Microsoft Online are regularly updated with the appropriate security updates for the software that they use. The time when updates are applied is based upon a timeline derived by the criticality, scope, and impact of the security vulnerability associated with each update.

Microsoft Online Services undergoes 3rd party penetration testing. Software undergoes appropriate testing and staging before being released into the Microsoft Online Services production environment to minimize impact to system integrity and availability.

Testing is performed against the OWASP Top 10:
https://www.owasp.org/index.php/OWASP_Top_Ten_Project

The Target Tracker team is able to review these tests under a non-disclosure agreement.

Intrusion detection systems provide continuous monitoring of all access to the SQL Azure services. Sophisticated correlation engines analyse this data to immediately alert staff of any connection attempts that are classified as suspicious.

iii. Access Controls

ECC employees will have access to customer data only for the purposes compatible with providing the contracted services. Such access is restricted to Target Tracker's directly employed programming and support team for such purposes as troubleshooting and in response to requests from customers.

Microsoft's virtual access to customer data is restricted based on business need by role-based access control, multi-factor authentication, minimising standing access to production data, and other controls. Access to customer data is also strictly logged, and both Microsoft and third parties perform regular audits (as well as sample audits) to attest that any access is appropriate. Microsoft engineers do not have default access to cloud customer data. Instead, they are granted access, under management oversight, only when necessary. They will use customer data only for purposes compatible with providing the contracted services, such as troubleshooting and improving features, such as protection from malware.

Access to the school data for customers 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/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.

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 cipher suites 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 cipher suite 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 cipher suite.
2. There is not a cipher suite 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.

Target Tracker employees access the CRM system using their own unique login and password. Each user profile is subject to user rights, permissions and privileges, ultimately controlled and managed by the Target Tracker system administrator. Activities carried out in the system are tracked within the database – being a standard feature of the CRM system.

The administrators employed by Target Tracker have administrator access to the CRM system. Under the support agreement in place with Target Tracker, the Avrion technical manager responsible for the CRM system also has administrator access to Target Tracker's customer database.

i. Disaster Recovery & Business Continuity

As a Category 1 responder, ECC, by obligations set by the Civil Contingencies Act (2004), is required to ensure business continuity plans are in place to ensure the continuance of key services even in an emergency, adopting and implementing business continuity management outlined in the international standard ISO 22301. EES for Schools plans for reasonably foreseeable events or situations that threaten our business, so we are able to continue to deliver an acceptable level of service to customers.

For the Microsoft Azure Cloud Services, we use to hold customer school data, we guarantee that as we deploy two or more role instances in different Update Domains, at least one role instance will have Role Instance Connectivity at least 99.95% of the time.

https://azure.microsoft.com/en-gb/support/legal/sla/cloud-services/v1_5/

Target Tracker's CRM resides on a dedicated private virtual server. An image is copied weekly and stored on separate hardware within the hosted infrastructure at the data centre. The database (data) including objects (documents, etc.) is backed-up daily and stored within the SAN environment, with automated status notifications. The notification monitors the success of the backup. Data backups are encrypted for protection purpose.

In the event of a disaster, the server image can be quickly restored to separate hardware within our hosted infrastructure and the latest data backup can be restored. User access to the restored system can then be resumed in the normal way.

**b. Data in Transit**

i. Software connections to the database

All connections between customers' software and the Target Tracker database are secure. All customer data in transit is encrypted. Microsoft Azure supports TLS 1.0, 1.1, 1.2. On Windows 10, with .Net 4.6.1, the protocol is TLS 1.2. For more detail, see:
https://www.ssllabs.com/ssltest/index.html

ii. Secure email

EES Software Operations actively discourages customers from using email to send any data potentially containing personal data, and provides alternative means of transfer. ecc does provide a means of encrypting emails for emails that we send, protecting and controlling sensitive information, with a full audit trail.

Emails sent within the CRM are transmitted via an authenticated SMTP Mail Relay Service, running on dedicated IP Addresses. The SMTP service uses a dedicated account registered to Target Tracker. This system is never used to send personal data.

iii. Secure Websites

All communication between Target Tracker and Microsoft Azure (SQL and Blob Storage) is encrypted (SSL) at all times. The Azure server certificate is always validated to prevent 'man in the middle' attacks.

Data can be transferred between customers and ourselves using a secure Website to which we can provide a temporary username and password. Data is encrypted in transit and at rest, but is only held on the site for as long as is necessary.

Support to schools is also provided using a secure web-based remote-connection tool from Logmein Rescue. Our technicians have individual logins requiring two-factor authentication via London Grid for Learning. For more on security of Logmein rescue, see: https://www.logmeinrescue.com/remote-support-features/security

The CRM system is accessed by a web browser. The site uses a 256-bit encryption SSL.

iv. Encrypted Hardware

All PCs and laptops on which school data might be processed are encrypted. All removable data devices on which personal data might be carried are encrypted.

**c. Data Retention and Destruction**

Data will be retained and deleted in accordance with EES for schools Data Retention schedules, as follows:

- General correspondence regarding named individuals: 2 years after contract end
- Named contacts and corresponding personal email address and mobile numbers: 2 years after contract end
- Pupil data for pupils over the age visible in Target Tracker software: Pupil data is held by Target Tracker for one full academic year beyond the years visible in the software. After that time it is expunged from the database. Customers, as data controllers, may wish to hold their own records for pupils beyond that.
- Pupil data beyond contract end: The data may form part of anonymised usage data for up to two years after contact end, or until the customer requests data deletion if sooner. Data is deleted 2 years after the contract is cancelled or on customer's request if sooner.
- Pupil data that has been provided to us for processing and adding to the customer database (e.g. at initial start-up): 1 full academic year from date of processing.

Any personal data or school assessment data will be deleted sooner than the schedule upon formal request.

Microsoft contractually commits to specific processes when a customer leaves a cloud service or the subscription expires. This includes deleting customer data from systems under our control.

- Should we terminate our cloud subscription, Microsoft will store customer data in a limited-function account for 90 days (i.e. the ‘retention period’) to give time to extract the data or renew our subscription.
- After this 90-day retention period, Microsoft will disable the account and delete the customer data, including any cached or backup copies. For in-scope services, that deletion will occur within 90 days after the end of the retention period.

When our customer data is hosted in the multi-tenant environments of Microsoft business cloud services, Microsoft logically separates customer data, helping prevent one customer’s data from leaking into that of another customer. This helps block any customer from accessing another customer’s deleted data.

If a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before Microsoft returns it to the manufacturer for replacement or repair. The data on the drive is completely overwritten to ensure that the data cannot be recovered by any means. When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.

Essex County Council purges and disposes of Hardware in accordance with HMG IA Standard 5 (IAS5).