Outcomes Star™ Online Information Governance Statement for Australia

Date of last update 11th August 2023

Contents

1. Introduction

This Information Governance Statement for Australia is the overarching policy for data security and protection for the Outcomes Star™ Online web application (hereby known as “the Star Online” or “the application”) in relation to users and organisations based in Australia.

The Outcomes Star Online is an asset of Triangle Consulting Social Enterprise Ltd (hereby known as “our” or “we”.)

2. Purpose and scope

The purpose of this statement is to:

- Demonstrate how the Star Online complies with relevant legislation, including:
    - the EU General Data Protection Regulation (2016) and the UK Data Protection Act (2018),
    - the Australian Privacy Act 1988 and Australian Privacy Principles ('APPs'),
    - the common law duty of confidentiality and all other relevant national legislation.
- Document our recognition of data protection as a fundamental right and our commitment to embracing the principles of data protection by design and by default.
- Document how we have implemented appropriate organisational and technical measures to uphold the policies in this statement, including following the Information Security Manual (ISM) and the Cloud Security Controls Matrix (CSCM) developed by the Australian Cyber Security Centre (ACSC).

The scope of this statement is:

- The Star Online web application – www.staronline.org.uk
- Triangle Consulting Social Enterprise Ltd. management of the application, including management of sub-contractors
- All data which we process in relation to the Star Online web application, which includes special categories of data.

3. Overview of Star Online web application

The Star Online system is an online web application supporting organisations to use the Outcomes Star™ by accessing Star resources, entering Star data and service user information, and reporting on this data. The Outcomes Star™ is a tool used under licence by services of various sectors, such as the health and social care sectors, to assess and support the progress that service users make in their lives whilst they are supported by the services.

The Star Online is owned and operated by Triangle Social Enterprise Ltd (company registration number 07039452, registered address Preston Park House, South Road, Brighton, East Sussex, BN1 6SB.)

Triangle work in partnership with Unique Outcomes (Registered Office: 3/3 Hanke Rd, Doncaster VIC 3108; ABN: 80 154 008 643) who have the exclusive licence to sell Outcomes Star™ licenses, training and consultancy to organisations in Australia and New Zealand.

Triangle sub-contract development and maintenance of the Star Online to Quality Education Solutions Ltd (company registration number 04700102, registered address Unit 3, Damery Works, Damery Lane, Woodford, Berkeley, GL13 9JR.) QES sub-contract the hosting of the Star Online servers to Microsoft Azure.

4. Underpinning policies & procedures

This policy is underpinned by the following:

- Triangle's Risk Register and Annual Statement of Internal Control – assesses all risks facing the organisation including to data security, information governance and 'clinical risk' (to service users) of the Star Online;
- Star Online Information Asset Register (IAR) and Record of Processing Activities (ROPA) – details the ways the Star Online stores and uses data, including the retention timetable;
- Star Online Helpdesk Data Security Procedure and Account Closure Procedure – sets out the rules and steps Triangle staff providing the Helpdesk service for the Star Online follow to comply with this statement;
- Star Online Emergency Incident Response Procedure – outlines the steps and communication required in any emergency incident relating to the Star Online including the reporting of any data security breach;
- Star Online Change Management Procedure – outlines the approaches taken by Triangle and our sub-contractors for the Star Online to ensure changes to the application are in line with this Data Security Policy;
- Star Online Disaster Recovery Procedure - outlines the procedures in the event of a security failure or disaster affecting digital systems including the Star Online and those necessary to the day to day running of our organisation;
- Star Online Governance Framework – outlines the lines of responsibility for managing the Star Online and the adherence to this Data Protection Policy;
- Star Online Data Security Programme – a programme of training for Triangle staff with privileged user roles for the Star Online;
- Star Online Role Based Access Model and Personnel List – documentation of Triangle and sub-contractor staff with privileged user roles;
- Star Online Anonymisation Policy – documentation of our approach to effective anonymisation and depersonalisation of personal and sensitive data;
- Triangle Information Security and Data Protection Policy - provides staff generally across Triangle with clear guidance on the collection, handling and disclosure of data collected whilst supporting organisations, and use of IT and devices.

We also regularly complete Data Protection Impact Assessments (DPIA) when making changes to any aspect of the Star Online or other services from Triangle involving the processing of personal data.

5. Star Online responsibilities and governance

The Star Online is overseen by the Executive Directors of Triangle in accordance with our Governance Framework, which involves monthly reporting, a minimum of a quarterly review and bi-annual planning and risk management.

In line with legislation, we employ a Data Protection Officer (DPO) who reports to the highest management level of the organisation:

- Name: Helen Bacon
- Job title: Implementation Manager
- Contact: Helen@triangleconsulting.co.uk

Please note, Helen is an interim DPO – we will be appointing an external specialist as DPO from January 2024.

We also have a Senior Information Risk Owner (SIRO) who manages risks associated with the Star Online and data security and contribute to the regular review of Triangle's Risk Register:

- Name: Sarah Owen
- Job title: Product Manager
- Contact: saraho@triangleconsulting.co.uk

6. Star Online sub-contractor management

Triangle sub-contract the capability to maintain, develop and host the Star Online so that we can benefit from the expertise, scale and governance of an external specialist organisation.

Before appointing a sub-contractor, Triangle will always undertake thorough due diligence when appointing a sub-contractor including accreditation to industry standards, references and testimonials. We will also conduct thorough tendering processes to ensure that sub-contractors demonstrate relevant experience and expertise. Triangle will also ensure that these processes apply to any sub-contracting that Triangle allow our sub-contractors to undertake (see below.)

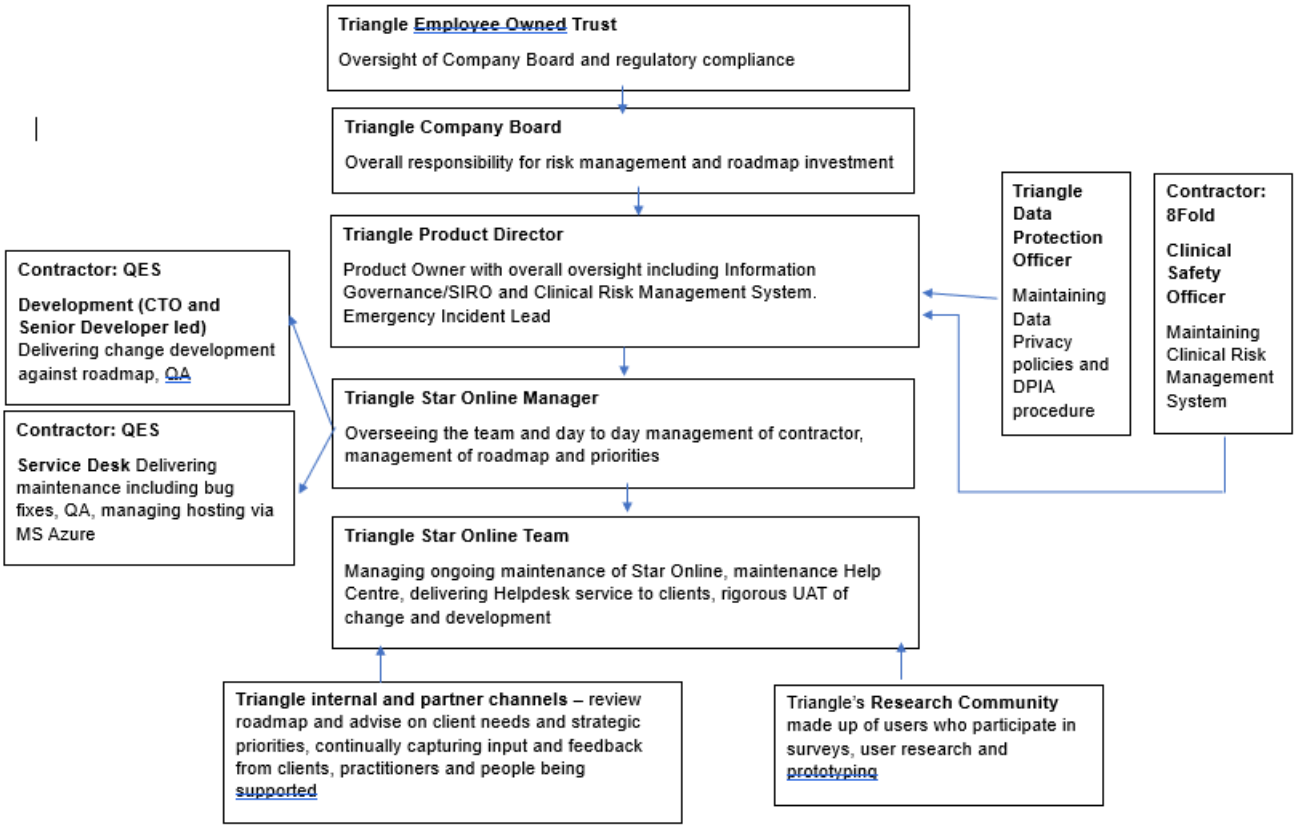
Triangle will always include specific requirements in a sub-contractor contract covering:

- Location of data and the servers and hosting of data to be held within the UK
- Compliance with GDPR and any other relevant data legislation
- Software design and management best practice including well-supported, up to date platforms and frameworks, and accreditation with relevant certification bodies
- Cyber security best practice including adherence to the UK's National Cyber Security Centre's 14 Cloud Principles and management of OWASP vulnerabilities
- A thorough procedure for identifying, reporting, responding and addressing any data or information security incidents
- Restrictions around sub-contracting, either completely or at least without prior approval of Triangle
- Performance and uptime expectations, including a guaranteed 99% uptime.

Triangle will closely manage all contracts including quarterly contract delivery review with the Executive Directors as part of our Governance Framework for the Star Online.

Star Online Governance Framework

Date of last update 16 June 2023



7. Star Online accreditation

Cyber Essentials is a scheme supported by the UK Government to ensure an organisation's use of hardware and software is secure and effective in the face of increased cyber security threats.

Triangle have Cyber Essentials certification, with external verification planned for January 2024.

QES have the following certification:

- ISO27001 – certificate number: 14123656
- ISO9001 – certificate number: 14131696
- Cyber Essentials Plus
- As an organisation they have N3/HSCN connections to the NHS pipeline (please note this is not currently used in conjunction with Star Online).

8. Star Online's Australian Privacy Principles (APP) Policy

This section sets out Triangle's data privacy approach and how we are compliant with the APPs.

A. Our approach to the APP's

In developing and reviewing our information governance policies for the Star Online, we have been informed by the APP's and APP Guidelines as issued by the Australian Information Commissioner issues under s 28(1) of the Privacy Act 1988 (Privacy Act) Australia.

We aim to recognise, respect and deliver the objectives of the Privacy Act:

- promoting the protection of the privacy of individuals
- recognising that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities
- providing the basis for nationally consistent regulation of privacy and the handling of personal information
- promoting responsible and transparent handling of personal information by entities
- facilitating an efficient credit reporting system while ensuring that the privacy of individuals is respected
- facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected
- providing a means for individuals to complain about an alleged interference with their privacy
- implementing Australia's international obligation in relation to privacy.

We identify Triangle as an APP Entity, as we are holding and storing an individual's information on behalf of our Australian client organisations.

Our Australian client organisations are organisations based in Australia who purchase training and licences for the Outcomes Star Online web app through Unique Outcomes and Triangle. These client organisations are also APP Entities, as they collect and use an individual's information using the Outcomes Star Online.

We identify that Triangle has an Australian link because Triangle carries on business in Australia and/or external Territories through our licensing agreement with Unique Outcomes and because the information hosted in the Star Online web app is collected from individuals who are physically present in Australia and external Territories.

B. The kinds of personal information the entity collects and holds

In compliance with APP 1.4(a), a full list of data stored on the Star Online database is set out in Appendix 1.

The data subjects (the individuals) that the Star Online holds information on are:

a) an employee of or an authorised representative of the client organisation with a Star Online account and who undertakes the role of the Account Lead;

b) an employee of or an authorised representative of the client organisation with a Star Online account and who are assigned a licence and login to the account by the Account Lead;

c) individual citizens that use services from the client organisation with a Star Online account, such as those provided in social care and health settings typically run by local authorities, charities, government or businesses.

Triangle does not have a direct relationship with the data subjects who are individual citizens, and these data subjects are not provided with direct access to our system.

Triangle holds legal agreements with the client organisations with a Star Online account governing their use of our outcomes tools and our system. This agreement creates the lawful and fair basis on which Triangle then hold and use the information collected by client organisations from individual citizens.

By accepting the terms of the agreement with Triangle, organisations agree to the storing and processing of data by Triangle and confirm their role and responsibility as an APP Entity.

This includes confirming that the collection of that data is being done in a lawful and fair way and in compliance with the APP, and if any exemptions apply under the 7 general permitted general situations, or the permitted health situations, or any other relevant exemption.

C. How personal information is collected and held

The personal information of individuals is collected by employees or other authorised representatives of a client organisation, either directly during support provision from the organisation with the individual, or a later point in time being transferred from a paper copy into the web app.

The client organisation is responsible for defining the processes and procedures through which these steps are achieved and their compliance with the APPs. Triangle support client organisations to comply with the APPs and other international data privacy legislation such as the GDPR with a privacy-by-design approach and specific features such as:

- The ability to disable fields and features if they are not relevant to the service
- The ability to identify dormant records and depersonalise them
- The ability to define and control user permissions using a Role Based Access Model (see Appendix 2)

If a client organisation is required to collect effective consent from an individual for the collection and storage of their data in the Star Online web app (and the client organisation is not applying an exemption under the 7 general permitted general situations, or the permitted health situations, or any other relevant exemption – see section D for more information) Triangle support this with several features including:

- Ready-made consent forms that explicitly inform the individual about what personal information is being collected, for what purposes, who can see that personal information and how to contact Triangle for any actions relating to that data.
- The ability to record and report on the provision of consent against a service user's record, including if consent was given from the individual or from another appropriate person
- The ability to upload a copy of a file relating to the provision of consent.

All data stored in the Star Online web app is made secure through a robust approach to cyber security, in line with the Australian Cyber Security Centre's Information Security Manual and the UK's National Cyber Security Centre Cloud Security Principles. It is also managed through comprehensive policies and procedures for the limited number of users with privileged user roles for the purposes of supporting client organisations to use the Star Online web app.

In all processing of personal data, we aim for data minimisation, ensuring that the data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Our policies and procedures ensure we use the least amount of identifiable data necessary to complete the work it is required for, and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

Where possible, we use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

D. Purposes for which the entity collects, holds, uses and discloses personal information

The Star Online's primary purpose is to hold and use personal information solely for the purposes of supporting client organisations to provide outcomes-driven services to their service users and to use outcomes data for service learning and improvement.

The Star Online's secondary purpose is to use completely and effectively anonymised data for learning and research about outcomes, service provision, our client organisations and our services. No identifiable personal or sensitive data (or data that can identify a service or organisation) is included in the delivery of this secondary purpose.

This secondary purpose is supported by the APP because the information is de-identified/anonymised before it is disclosed, and it is directly related to the primary purpose and because it relates to a permitted health situation for health and well-being research.

See below and our Anonymity and Depersonalisation Policy which is available separately.

E. Our approach to anonymity and pseudonymity

The Star Online web app is built around a service in a client organisation providing person-centred, holistic, and personal support over a length of time. As core elements of the Star Online web app interface are designed to be shared with a service user, for example by sharing screens in a support session, or sharing a download of their latest information, Triangle support and recommend that names are recorded in the Star Online web app. We believe this to be a reasonable use of personal data and that not using names can make it impracticable for client organisations to provide support to individuals.

However, we do also allow organisations to disable key demographic fields, including first name, surname, date of birth, and contact details. Even with this setting applied, Triangle approach the rest of the information about an individual as personal and sensitive data as it does not meet our criteria for depersonalised data. A unique ID must be entered for each record which can act as a pseudonym.

The responsibility for deciding on whether to enable or disable these key fields, and how to use the unique ID as a pseudonym, is with the client organisation and their responsibilities are clearly set out in the legal agreement between them and Triangle.

Where Triangle need to use the personal information of service users and authorised personnel from client organisations, for either the primary or secondary purposes of the Star Online web app, we ensure the data is fully and completely anonymised. For information on this can be found in our Anonymity and Depersonalisation Policy.

F. Consent for collection of personal and sensitive information

Triangle do not collect information directly from individuals. It is collected by our client organisation who is another APP entity and then stored in the Star Online. A client organisation accepts responsibility for ensuring that the personal and sensitive information they collect is reasonably necessary for, or directly related to, the organisation's functions or activities.

Triangle accept responsibility for ensuring that the personal and sensitive information collected and stored in the Star Online is only used for our primary and secondary purposes as set out in section D and in a lawful and fair way. This limitation of use is defined and controlled by the legal agreement signed between Triangle and a client organisation.

As the Star Online stores sensitive information about an individual, we recognise that APP 3.3 imposes the requirement that unless an exemption applies, an APP entity must both satisfy the above criteria and that the individual about whom the sensitive information relates must consent to the collection.

Compliance with this requirement is the responsibility of the client organisation collecting the information from the individual. If an exemption does not apply, then Triangle support organisations to manage the collection of consent with features set out in section C.

If one of the 7 permitted general situations as listed in Privacy Act s 16A apply, or one of the permitted health situations apply, then the specific features relating to service user consent set out in section C can be disabled in the Star Online web app by a client organisation.

Under the terms of the GDPR in the UK:

- The lawful basis for processing data belonging to employees of an organisation with a Star Online account is contract, and separate consent is therefore not required.
- The lawful basis for service user data is legitimate interest as we process service user data to fulfil our contractual obligations to an organisation with a Star Online account and do not have a direct relationship with service users.
- The organisation purchasing the Star Online account is responsible for identifying an appropriate lawful basis on which data is collected and stored in the Star Online.

G. Dealing with unsolicited personal information

The Star Online does not allow client organisations to customise or configure the data fields or data types collected by the Star Online. This means that the data collected will always directly relate to our stated primary and secondary purposes.

H. Notification of the collection of personal information

Triangle do not collect information directly from individuals. It is collected by our client organisations who are separate APP entities and then stored in the Star Online. A client organisation accepts responsibility for ensuring that they are complying with the APPs with any notification required for the individuals from whom information is being collected.

Triangle support client organisations with this responsibility with features set out in section C.

I. Direct marketing

Triangle do not undertake any form of direct marketing using the personal information held in the Star Online web app. Triangle do not use the personal data of service users as collected by authorised personnel from client organisations for any communication purposes. A client organisation is responsible for ensuring that they only use the personal of service users collected by them and stored in the Star Online web app in a lawful and appropriate way.

Triangle's legal agreement with a client organisation ensures that we will only use the personal information (email address) of authorised personnel with a login for the client organisation's Star Online account for the purposes of supporting that client organisation to use the Star Online (our primary purpose.)

J. Cross-border disclosure of personal information

Triangle are based in the UK. Triangle's sub-contractors are based in the UK. The Star Online's servers are hosted in the UK.

When a client organisation records personal information about service users in the UK, that data will be disclosed to Triangle in the UK.

For clarity, we are calling this a 'disclosure' but the terms of the legal agreement or contract between a client organisation and Triangle limit Triangle's use of this data to only uses that meet our primary and secondary purposes as set out in section D. In the APP guidance, it states that it will be

a use and not a disclosure if a contract "gives the other entity effective control of how the personal information is handled by the overseas recipient." The client organisation retains the right and power to access the information and to change or retrieve it, including the ability to retrieve and permanently delete this information when no longer required at the end of the contract.

Triangle's sub-contractors, QES Ltd and Microsoft Azure, are also based in the UK and their use of the data is completely controlled and limited to the terms of their agreements with Triangle, including the rights and abilities set out above.

In addition, the APP guidance status that an APP entity may "disclose personal information to an overseas recipient where the entity reasonably believes that the overseas recipient is subject to a law that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way the APPs protect the information." As Triangle and our sub-contractors are completely based in the UK in terms of our processing of data relating to an Australian client organisation, that activity is covered by the EU General Data Protection Regulation (2016) and the UK Data Protection Act (2018), which is substantially the same as the APPs.

As set out in Section A, Triangle have identified an 'Australian link' and under the terms of the APP and Australian Privacy Act, would be an APP entity. This means that Triangle are accountable for the personal information disclosed to us as an 'overseas recipient' from Australia and external Territories, and the originating APP entity (a client organisation) is not accountable for any breach of this policy or legislation undertaken by Triangle or our sub-contractors.

K. Adoption, use or disclosure of government related identifiers

Triangle do not collect information directly from individuals. It is collected by our client organisations who are separate APP entities and then stored in the Star Online. A client organisation accepts responsibility for ensuring that they are complying with the APPs in terms of the information being collected, therefore it is the responsibility of the client organisation to ensure any collection or use of government identifiers is compliant.

Triangle support client organisations with this responsibility by not directing users to include a specific type of identifier.

L. Quality of personal information

Triangle do not collect information directly from individuals. It is collected by our client organisations who are separate APP entities and then stored in the Star Online. A client organisation accepts responsibility for ensuring that they are complying with the APPs in terms of the information being collected, therefore it is the responsibility of the client organisation to ensure personal information is accurate, up-to-date and complete.

Triangle support client organisations with this responsibility through a number of features including easy to use lists of records, editable fields and guided processes for updating data, ready made reports and a Helpdesk service for support.

M. Security of personal information

Triangle ensures the security of the personal information stored on the Star Online through several different approaches.

These include a robust cyber security approach in line with the UK's National Cyber Security Centre's Cloud Security Principles and the Australian Cyber Security Centre's Information Security Manual. See section 9 for more information.

In addition, the service provided by Triangle and the services Triangle contract from QES Ltd and Microsoft Azure are controlled by a comprehensive set of documented procedures, including for training and education.

The Star Online has a clearly defined retention policy that allows client organisations full control over their data at the end of their contract with Triangle.

Whilst a Star Online account is active, the data within it is retailed unless the organisation or users remove or change it using the auditable data change features available with the Star Online. Where users cannot directly delete or change data from the user interface of the Star Online, there are procedures to enable the organisation to request this of the Star Online Helpdesk service provided by Triangle.

When a Star Online account is closed, Triangle will automatically fully and effectively anonymise all data in the account 3 months after the agreed closure date in accordance with our Anonymisation Policy. The data will then no longer be classed as personal data and will be stored by Triangle indefinitely to support our programme of research and learning around outcomes.

Organisations are given the opportunity to opt out of the anonymisation and for their data to be permanently and completed deleted 3 months after the agreed closure date.

N. Accessing and correcting personal information

We uphold the personal data rights outlined in the GDPR:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

As Triangle do not have a direct relationship with the data subjects who are individual citizens, we enact these rights through providing services to and working with the Account Lead, following our detailed Helpdesk Data Security Procedures documentation.

9. Star Online security architecture and controls

This section sets out the technical set up of the application and how that delivers data security. We aim to comply with the UK National Cyber Security Centre's Cloud Principles (https://www.ncsc.gov.uk/collection/cloud-security) and with the Information Security Manual (ISM) and the Cloud Security Controls Matrix (CSCM – March 2022 version) developed by the Australian Cyber Security Centre (ACSC).

Each heading in the following section corresponds to information required for the CSCM and references the relevant ISM Principles across Govern (G), Protect (P), Detect (D), Respond (R.)

A. Governance and Chief Information Security Officer

G1: A Chief Information Security Officer provides leadership and oversight of cyber security

G2: The identity and value of systems, applications and data is determined and documented.

G3: The confidentiality, integrity and availability requirements for systems, applications and data are determined and documented

G4: Security risk management processes are embedded into organisational risk management frameworks

G5: Security risks are identified, documented, managed and accepted both before systems and applications are authorised for use, and continuously throughout their operational life

Triangle's Senior Information Risk Officer acts in the same role as the Chief Information Security Officer, providing cyber security leadership and guidance.

The SIRO oversees Triangle's cyber security approach and ensures compliance with policies, standards, regulations and legislation. Triangle's SIRO works closely with the Chief Technology and Information Security Officer at our sub-contractors QES Ltd.

The SIRO is responsible for monitoring the performance of our cyber security approach and training programme, regularly reviewing policies and documentation, and our security risk management activities.

The SIRO leads on cyber supply chain risk management activities for Triangle, and leads on the management of any cyber security or information governance incident, following our incident management procedure. The SIRO reports to the senior leadership of Triangle through the Star Online Governance Framework, including a biannual update of the Risk Register.

B. Cyber supply chain risk management

P1: Systems and applications are designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.

P2: Systems and applications are delivered and supported by trusted suppliers.

P3: Systems and applications are configured to reduce their attack surface.

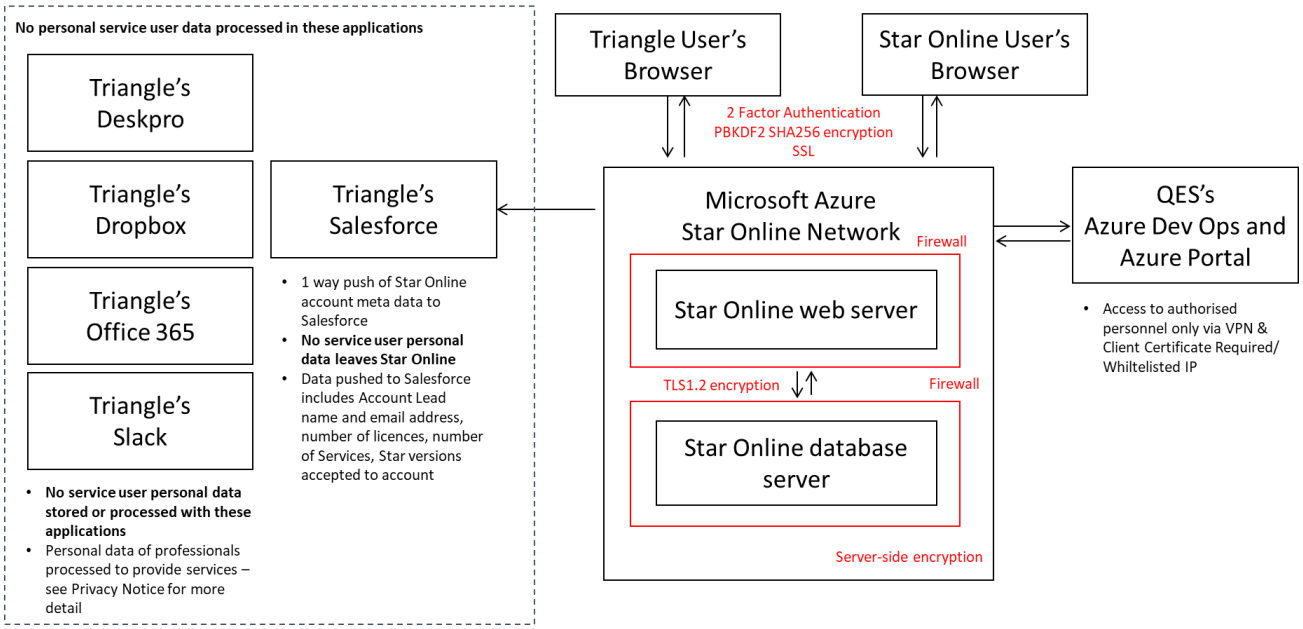
See Section 6 for more information on how Triangle manage the cyber supply chain. This process effectively creates a shared responsibility model, where security and information governance responsibilities are documented and signed up to across the full supply chain and our client organisations.

Triangle ensure that the contractual arrangements with sub-contractors document the security requirements associated with the confidentiality, integrity and availability of data entrusted to them, the right to verify compliance (which is exercised on a regular basis), the types of data and its ownership, the regions where data will be processed, the access to audit logs, and a policy for backups and resilience. There is a minimum notification period for the cessation of any services and if any authorised activity takes place, this will trigger Triangle's incident procedure.

This is a systems diagram, showing the relationship across Triangle's cyber supply chain and the flow of personal and sensitive information.

Triangle and Star Online systems diagram

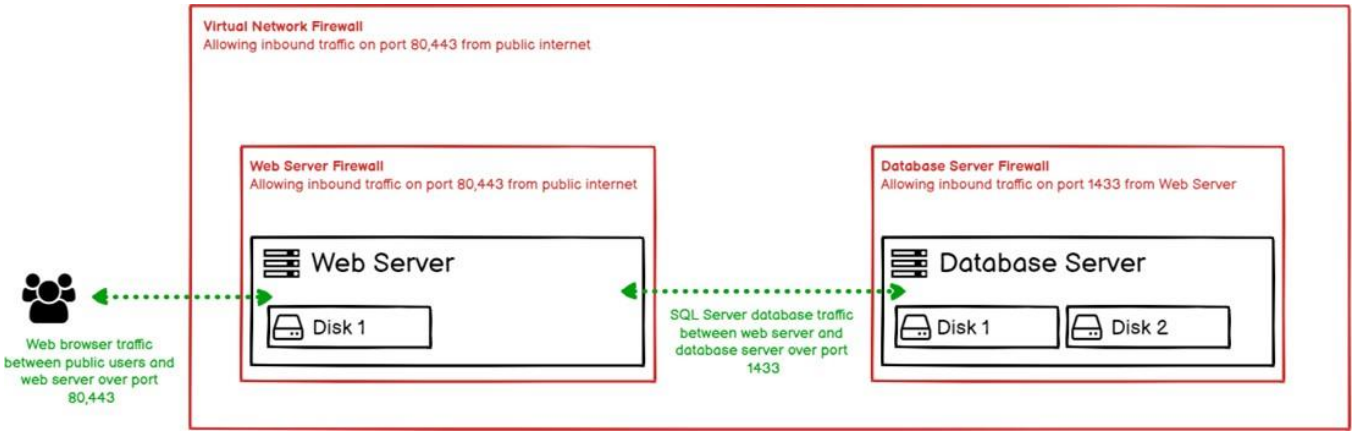
Date last updated 26th April 2021



C. Application hardening

Triangle and QES are committed to secure-by- design principles and secure programming practices.

Overleaf is technical configuration diagram, showing the various technical settings that been applied to the Star Online web app and infrastructure.



D. System administration

P4: Systems and applications are administered in a secure and accountable manner.

Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualized within unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. The administrative infrastructure is segregated from a wider network.

We utilise a dedicated devices for service administration approach in line with UK National Cyber Security Center guidance, with a dedicated machine for service management that QES use to access the host devices that run the Star Online application. This machine has restrictions in place to limit the use to only service management action and has the same security settings that apply to the Star Online and other applications that QES manage that are also used by public sector organisations and so require the same security architecture and permissions.

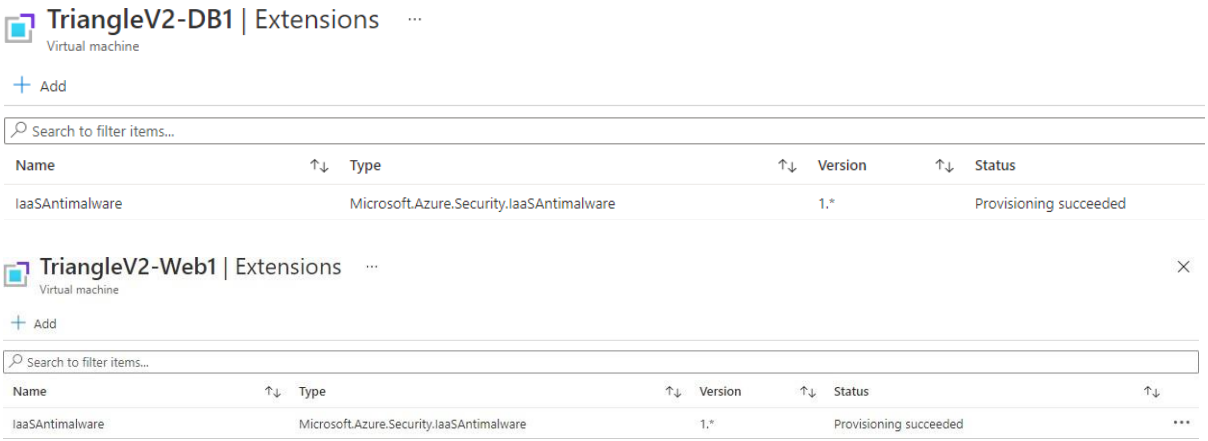
E. Vulnerability management and intrusion prevention

P5: Security vulnerabilities in systems and applications are identified and mitigated in a timely manner.

Our servers have built in Denial of Service attack (DDoS) protection. Azure monitor and inform us of any suspicious activity (intrusion detection) on the server and we have built custom proactive monitoring alerts that will notify of immediate or impending service failure, or suspicious activity to be investigated.

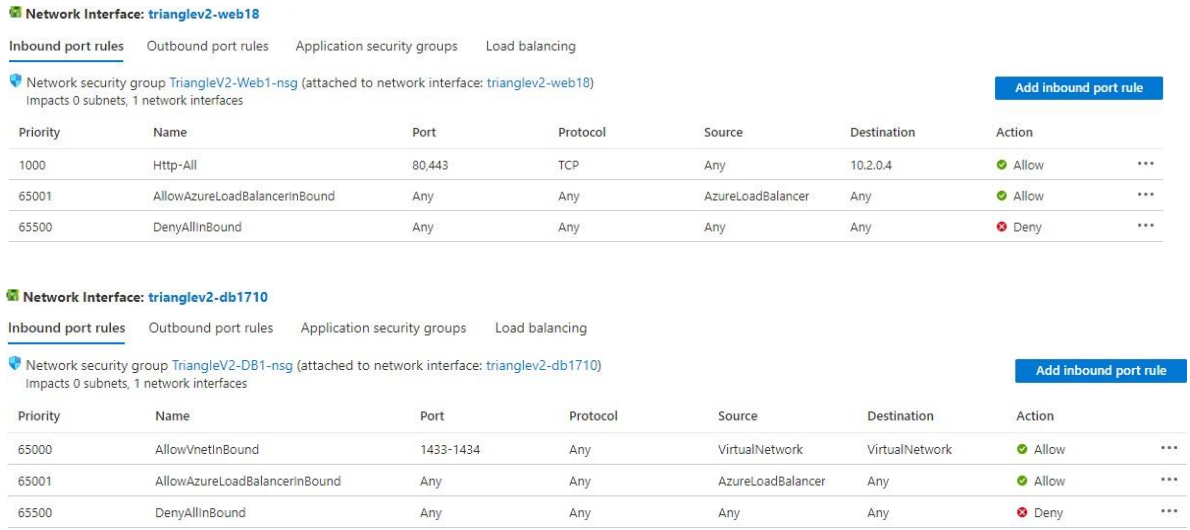
A penetration test is completed on the application annually by an external specialist. The most recent pen test was completed in August 2021 by the NCC Group. A summary of results is available separately on request.

The system uses Microsoft Defender Antimalware managed through Microsoft Azure.



Firewalls are managed through Microsoft Azure. All open ports and services have been subject to justification and approval by an appropriately qualified and authorised business representative, and this approval has been properly documented.

There are policies in place to ensure that all firewall rules that are no longer required are to be removed or disabled in a timely manner, and there are currently no open ports or services that are not essential for the business.



The remote administrative interface has been disabled on all firewall devices. Only web traffic is enabled on the Triangle Application Server. Only SQL Server ports are enabled from inside the virtual network on the database server.

F. Patch management

We have a dynamic approach for patch management:

- Critical, low risk updates to the server automatically take place the day they are issued by Microsoft. All other updates are tested on our STS and UAT environment prior to release.
- Application patches are tested in the same environments prior to a production release.
- OS Host updates are managed using Azure Update Management and scheduled during agreed maintenance windows with Triangle.

G. Data in transit and at rest protection

P7: Data is encrypted at rest and in transit between different systems.

All transportation of data between application and database is done over a TLS1.2 encrypted channel. The Star Online will not support TLS1.0 from March 2022.

Our application uses PBKDF2 and SHA256 encryption and benefits from server-side encryption using Service-Managed keys through Microsoft Azure.

H. Data backup, restoration and service continuity

P9: Data, applications and configuration settings are backed up in a secure and proven manner on a regular basis.

Triangle guarantee an uptime of not less than 99.9%.

We guarantee a transfer time/speed target of less than 4 seconds on average for end users of the Software located in the UK and aim for a transfer time/speed target of less than 4 seconds of average for end users of the Software located outside of the UK.

We ensure that scheduled downtime is managed at minimal disruption to users and outside of working hours as much as possible.

We actively monitor system uptime, server resource use and performance using automated monitoring alerts and respond to any alerts using our Incident Response Procedure.

The Star Online has a Disaster Recovery Procedure (DRP) in place for and the process of restoring code from the code repository and data from the backup is regularly used.

Recovery point objective

The database runs under a backup policy that ensures in the event of a complete system failure, the maximum amount of data loss that could occur is never data older than 5 minutes.

A full backup of the database is taken weekly, with incremental log file backups taken every 5 minutes. Database backups are stored on a rolling 30 day period.

Recovery time objective

The contracted RTO to Triangle is 24 hours. The server has been configured with the Azure Site Recovery feature, meaning we have an idle secondary server in a separate datacentre that we can recover service to within 15 minutes. (The last test of this took 8 minutes).

In the case of a full datacentre failure, the service would be reinstated to within 5 minutes of when the event occurred. Return to service time will be <1 hour.

I. Access to systems and their resources

P10: Only trusted and vetted personnel are granted access to systems, applications and data repositories.

P11: Personnel are granted the minimum access to systems, applications and data repositories required for their duties.

See Appendix 1 for a description of the Role Based Access Model in use. A full breakdown of current personnel and their access to privileged user roles for the application is available on request as this

breakdown is continually monitored and updated. Star Online Manager/SIRO manages access to privileged security roles as part of Triangle's JML (joiners, movers, leavers) policy.

QES store all data for each system they maintain in distinct, separated databases, with unique SQL logins. There is no possibility of any data being shared from other systems as a result of this architectural approach.

On the Star Online, all data is restricted to each individual account. QES and Triangle take data security seriously with any staff able to access data in an account trained in data security procedures.

J. Cyber security awareness training

P13: Personnel are provided with ongoing cyber security awareness training.

As part of QES's readiness programme, QES has specifically upskilled staff in two areas; GDPR readiness and CREST Technical Application Security testing, enabling us to better understand and implement defensive measures against threats to data security and integrity. All staff have been trained and made aware of GDPR and the ICOs Think.Check.Share guidance. All QES staff are DBS checked.

Triangle staff with access to data within Star Online accounts via privileged user roles is limited to the helpdesk. Helpdesk staff undertake regular training in data protection and security as part of the Star Online Data Security Programme using modules built from from the ICO and National Cyber Security Centre guidance.

K. Authentication hardening

P12: Multiple methods are used to identify and authenticate personnel to systems, applications and data repositories.

Multifactor authentication for all users

Two Factor Authentication is enabled. In addition to the username and password, users are sent a one-time access code by email when they login every 24 hours and per unique IP address. This must also be entered before a user is authenticated with the system.

Strong passwords

Star Online requires strong passwords (minimum 8 characters, including upper case, numerical and special character) and enforces a new password every 3 months.

User Accounts are managed directly by organisations within their accounts.

All user accounts require 2 factor authentication every 24 hours.

L. Facilities and systems

P14: Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel.

The Star Online is hosted on Microsoft Azure servers. Azure primary datacentre is in South West, UK. Azure secondary paired datacentre is in South, UK, giving us full Geo-Redundant Storage.

The server configuration is mirrored between two hypervisors, with automatic failover between the two in event of hardware failure. All data is stored on a fully redundant Storage Area Network.

Access to Microsoft Azure servers is limited by location and only approved individuals. Microsoft Azure provide us with a private cloud offered over a private internal network. Azure holds industry standards including CSA STAR Certification, ISO 27001, ISO 27017, ISO 27018, ISO 20000-1, ISO 9001, HIPAA, FedRAMP, SOC 1, SOC 2, UK G-Cloud.

M. Web application development

Adherence to the OWASP Application Security Verification Standard is mandated by our contractual agreement with our sub-contractors, QES

Change to the system is managed as per our Change Management procedure, and we adhere to security by design principles. All Star Online content is offered exclusively using HTTPS, and validation or sanitisation is performed on all input handled by the Star Online.

The application is periodically tested for vulnerabilities by a permanent member of the development team who has been trained in CREST Ethical Hacking and penetration testing. QES development team run monthly “Hackathons” whereby they attempt to hack into our application in a test environment which mimics that of the production environment. The findings of this are then fed into the development sprints for remediation.

The software is also continually tested using our automated testing model through TFS Build and Release. Through continuous integration (DevOps and DevSec) we are able to use established tools which specialise in checking for vulnerabilities but also build our own custom tools which run every time we make a change to the system.

An example of a few we have integrated:

- SonarQube - a code quality tool which checks for bugs and vulnerabilities in the code in line with OWASP. (https://www.sonarqube.org/)
- OWASP ZAP (Zed Attack Proxy) – Vulnerability scanner (https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)
- Custom built – API anonymous scanning – Ensures that there are no vulnerable APIs
- Custom built – Web.config checks – Ensures all security keys are enabled.

N. Event logging and monitoring

D1: Event logs are collected and analysed in a timely manner to detect cyber security events.

D2: Cyber security events are analysed in a timely manner to identify cyber security incidents.

All server administration actions are audited in Azure and a full application audit history stored in the system database.

Full audit logs for all activity in an account are available on request from the Star Online Helpdesk. Account Lead to email the Helpdesk and make a request for the audit log or specific activity within the audit log for your account. Data will be shared via a secure file sharing service specified by the client organisation or made available within the interface of the Star Online account.

Currently, only the development team at QES and those with Super User access at Triangle are able to view the audit log. The data in the audit log cannot be amended. Audit logs are retained for as long as the account is active.

See Appendix 3 for more information.

O. Detecting, managing and reporting cyber security incidents

R1: Cyber security incidents are reported both internally and externally to relevant bodies in a timely manner.

R2: Cyber security incidents are contained, eradicated and recovered from in a timely manner.

R3: Business continuity and disaster recovery plans are enacted when required.

Triangle maintain a cyber security and data privacy incident register which covers the dates of the incident (occurred, discovered, communicated, resolved), the details of the incident (source, causes, actions, remedial steps and lessons to take forward.) All incidents are managed by the SIRO.

In the case of an emergency incident, Triangle's Emergency Incident Response Procedure would be followed. Full information is available as a separate document, but in summary this procedure involves:

- Alerting the primary emergency incident contacts at Triangle and QES immediately - QES will acknowledge any notifications of business-critical incidents within 1 hour. (Please note, QES are available during UK working hours only. Triangle maintain a 24 hour emergency contact which is available for Unique Outcomes staff in the case of an emergency outside of UK working hours. Client organisations based in Australia should contact Unique Outcomes as the first point of contact.)
- Ongoing communication with clients affected by the incident through the Helpdesk.
- Work within the decision framework set out in the Disaster Recovery Plan.
- QES will aim to resolve the service being unavailable within 1 working day, or within 5 days for other business critical issues.
- All fixes and resolutions including restoring the system will be discussed with Triangle, thoroughly quality assured and tested by QES' testing team and tools and signed off by Triangle before implementation.
- Documentation of the issue in Incident Report including thorough investigation into the incident, analysis of action taken, sequence of events, learnings taken forward.
- Review and discussion of Incident Report at Executive level including the communication to relevant authorities (such as reporting to the UK Information Commissioner's Office) and to the data subjects affected.

P. Data sanitisation

All data from Star Online accounts is held in the cloud and no data is stored on Triangle or QES devices. All devices used by Triangle and QES are securely sanitised at the end of their life using a Secure Erase Wipe Method or similar.

Whilst a Star Online account is active, the data within it is retailed unless the organisation or users remove or change it using the auditable data change features available with the Star Online. Where users cannot directly delete or change data from the user interface of the Star Online, there are procedures to enable the organisation to request this of the Star Online Helpdesk service provided by Triangle.

When a Star Online account is closed, Triangle will automatically fully and effectively anonymise all data in the account 3 months after the agreed closure date in accordance with our Anonymisation Policy. The data will then no longer be classed as personal data and will be stored by Triangle indefinitely to support our programme of research and learning around outcomes.

Organisations are given the opportunity to opt out of the anonymisation and for their data to be permanently and completed deleted 3 months after the agreed closure date.

Q. Device security

All devices at QES are protected with Microsoft Defender Antimalware and company policies such as encryption, email filters, web traffic control, and portable device ports locked down.

Triangle devices are protected in line with the following illustration from our IT security provider, It's What's Next (Milton Keynes) CIC:

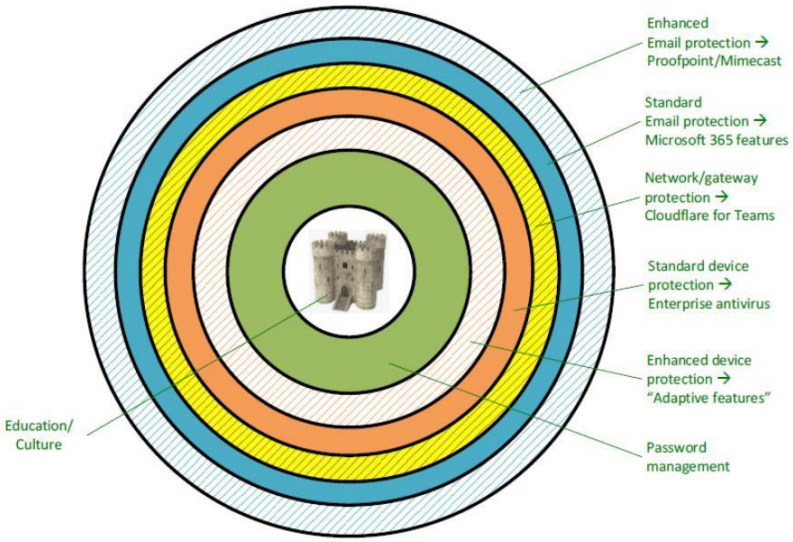


Figure 1: IWN-IT Layered Cyber Security Framework illustration

In addition to the security settings applied above, acceptable use policies ensure that staff use good practice including preventing the use of public WIFI or personal devices for all QES and Triangle's Star Online Team personnel for accessing the application via a privileged user role.

10. Review

This document will be reviewed and updated by 5th August 2024, or earlier if the planned changes to the Australian Privacy Act are finalized and made legislation before that time.

Appendix 1: Star Online and Role based access control (RBAC)

Security role	Permissions and access
Azure Network Administrator	• Manage security settings including firewall, incident monitoring and patch updates
System Administrator	• Create, Read, Update, Delete (CRUD) in SQL databases for Live and development environments • CRUD codebase of application – Live and development environments - in Azure Dev Ops • Push releases
Quality Assurance	• Read only in SQL databases for Live environment • CRUD for SQL databases and codebase in Development environments
Super User	• CRUD Star frameworks, lists, post-login pop up and broadcast notifications • CRUD Help Centre content
Super User – Training environment	• CRUD Scenarios in Training site
Helpdesk	• CRU Accounts, Edit licences available to Accounts • CRUD Users • CRU data in all Accounts and Delete for specific data including actioning service, engagement, user deletion requests
Account Lead (Client role)	Within authorised Account: • Accept Star frameworks • Create and edit Services • Create and edit Users including deactivating users • View and edit all data including actioning Star and service user deletion requests
Service Manager (Client role per service)	Within authorised Service: • Create and edit Users • View and edit all service user data including actioning Star and service user deletion requests • View Star resources
Practitioner (Client role)	Within authorised Services: • View and edit service user data • View Star resources
Licensed Trainer (may also be other client roles)	• View Star Training resources in Live environment • Access Training environment and set up training sessions using existing scenarios

Appendix 2: Data stored on the Star Online

All users of the Star Online must provide a valid email address, password, first name and last name in order to log in and gain access to the application and resources it contains.

Organisation name, type and location is also recorded and we collect some activity in order to support use of the system, e.g. the date and time of the last login.

In addition to the information we hold on all active Star Online users, we hold the service names, service types, locations of users. We also record their activity within the system, for instance, the last time they logged in, and if, when and for which client they've entered Star readings and action plans or requested Star readings be deleted.

Information the Star Online system will process on service users is set out below.

Service user information

Service user records are created and managed by organisations using the Star Online, there is no 'service user' user account type and so we don't require or use an email address or password for service users.

Personal data relating to service users can be stored securely within the system, including:

- First name and Surname and/or Unique ID reference
- Preferred name (optional)
- Service names and Star versions being used with that individual
- Start and end dates of support (engagements)
- Star readings, completion information and Notes – see below for more information
- Action Plans and Other Notes (optional) – see below for more information

The following information can be added to the service user record:

- Address (optional)
- E-mail address (optional)
- Phone (optional)
- Gender (optional)
- Ethnicity (optional)
- Support needs (checkboxes are provided relating to the likely support needs depending on the Star used with a service user)

All these fields are optional, so they can be left blank. If the same information is stored in another system or the Star Online isn't used for reporting it may not be necessary to also capture the information on the Star Online service user record and organisations.

Star readings

Organisations can enter multiple Star readings for service users. For each Star reading, there are a number of areas covering the different aspects of a person's life. For each area there are a series of numbered statements describing where the service user might be – text descriptions of the person's

current situation, behaviour and attitudes – from which the worker and service user collaborate to make a choice. Notes can be entered in free text fields for each area to enable workers to expand on the "reading" selected.

Action plans

The Star Online action plan feature is optional. It enables workers to record notes in a free text field about one or many areas of the Star and automatically includes the "reading" number selected for each area included in the action plan.

Other Notes

This feature allows other related data to be stored against a service user's record and engagement, such as number of other individuals in their household or school attendance figures. Currently this feature is being piloted and only available to a small number of organisations. Access to each Other Notes type is controlled by the Helpdesk and all are disabled as default.

Appendix 3: Audit log and list of events

User log in success

User updated

User created

User password reset

View user

Lookup value updated

User log in failed

User password updated

Account viewed

Account created

Account updated

Account Frozen

Account Blocked

Account deleted

Audit details viewed

Audit list viewed

Star type viewed

Star type created

Star type updated

Star type deleted

Account activated

Service viewed

Service created

Service updated

Service deleted

Service deactivated/archived

Star type distributed

Service user viewed

Service user created

Service user updated

Service user deleted

Engagement created

Engagement ended

Engagement updated

Star entry created

Star entry updated

User profile updated

User profile viewed

User licence deactivated

User licence reactivated

User deleted

Data request created

Data request viewed

Data request completed

Data request cancelled

Data request rejected

Data request approved

User session error