TORO DIGITAL

TECH MADE SIMPLER

SAFER Defence

SERVICE DESCRIPTION

Table of Contents

1 Service Overview.

SAFER Defence - A Human Risk Awareness and Behavioural Resilience Capability for UK Defence.

2 Service Description.

SAFER Defence is a secure, always-on mobile awareness and decision-support service designed to strengthen human-layer resilience across the Defence Whole Force.

The service provides Defence personnel, contractors and approved users with timely, trusted guidance at the point of need, supporting safer and more consistent behaviours in a complex threat environment.

SAFER Defence delivers real-time awareness across multiple human risk domains, including cyber and digital behaviour, health and safety, mental wellbeing, AI use, and home and family digital resilience.

The service complements existing Defence training and communications by providing continuous behavioural reinforcement between formal learning events. It does not replace mandated training, but supports sustained awareness and judgement in day-to-day activity.

SAFER Defence is delivered as a secure, supplier-operated SaaS capability under G-Cloud 15 Lot 2b (SaaS). Content can be configured to organisational context, enabling consistent use across Defence establishments while allowing local tailoring where required.

The service is designed to scale across Defence and to adapt as threats, technologies and assurance expectations evolve.

3 What the Service Does.

SAFER Defence provides a mobile and web awareness and decision-support capability that delivers practical guidance and behavioural reinforcement in the flow of life.

The service enables users to access real-time, Defence-aligned guidance at the point of decision, supporting safer cyber and digital behaviour, improved safety awareness, and more informed use of emerging technologies such as AI.

The service delivers short, service-relevant awareness content designed to be quickly consumed and easily recalled in operational environments.

SAFER Defence provides continuous behavioural reinforcement through proactive prompts and updates, supporting cultural consistency rather than one-off compliance activity.

The service incorporates intelligence-led updates, to reflect emerging threats, changing risk patterns and updated guidance at Official.

The service is modular and can be extended over time to support additional awareness domains, including service and organisational culture, specialist hazards, environmental responsibilities and role-specific requirements.

The service complements existing Defence training and assurance activities by reinforcing expected behaviours between formal learning events.

4 Who the Service Is For.

SAFER Defence is designed for use across the Defence Whole Force.

The service is suitable for military personnel, civil servants and Defence contractors who require timely, trusted guidance to support safe and consistent behaviour in complex operational and digital environments.

The service can also be used to support awareness for industry partners, visiting personnel and other authorised users operating within Defence establishments, where appropriate.

SAFER Defence is suitable for use across Defence organisations, including headquarters, bases, stations, ships, units and deployed environments.

The service is designed to operate at Official level and provide inclusive access to practical, operationally relevant guidance for all users, including those without consistent access to issued IT or easy access to Defence policy or training. It delivers concise, accessible and policy-aligned guidance in a format suitable for real-world operational use.

The service supports a Whole Force approach by enabling consistent awareness and behavioural reinforcement across permanent staff, transient workforces and partner organisations.

5 How the Service Is Used.

Users access SAFER Defence via dedicated mobile app (iOS/Android) or web browser on personal devices (BYOD) or MOD devices (domain whitelisted) to receive practical guidance, proactive insights and short awareness content in the flow of life.

The service can be used on base, deployed (with internet connection), or at home, supporting consistent awareness regardless of location or working pattern.

SAFER Defence uses Supplier-managed AI-enabled services delivered using third-party AI software-as-a-service technology hosted in UK or trusted environments solely for content retrieval and contextual awareness support. AI does not perform autonomous decision-making, store personal data on devices, or access MOD corporate systems.

SAFER Defence operates as a three-mode human resilience system, delivered through an AI-enabled platform. Each mode addresses a different human risk failure point, together providing comprehensive coverage.

5.1 Reactive use.

Reactive use provides just-in-time judgement support. Users can ask questions at the moment uncertainty or risk arises, based on a real decision or situation they are facing.

The service responds using a curated, assured knowledge base aligned to Defence policy and guidance, rather than open internet sources. This ensures responses are consistent, appropriate to Defence contexts, and suitable for operational use.

5.2 Proactive use.

Proactive use supports structured, self-directed understanding. Users can explore themes, topics and awareness areas when relevant to their role or circumstances, rather than at fixed training intervals.

The service enables guided exploration and role-aware framing to support deeper understanding and confidence over time.

5.3 **Delivered use.**

Delivered use provides timely behavioural reinforcement through a Message of the Day approach.

Short, relevant prompts and insights are delivered to users to reinforce expected behaviours and raise awareness before issues occur.

This mode focuses on behavioural nudging and reinforcement rather than formal training.

Together, these three modes enable SAFER Defence to support consistent, practical and scalable human risk awareness across the Defence Whole Force.

6 **Service Delivery Model.**

SAFER Defence is delivered as a secure, supplier-operated software-as-a-service capability within a single, centrally governed platform environment.

The service is designed to operate as one Defence-wide capability, providing consistency, scalability and efficient management across organisations, while avoiding the fragmentation associated with multiple standalone tools.

Within the SAFER Defence environment, context-specific AI agents and associated knowledge banks are deployed to reflect different Defence operating contexts, such as Land, Maritime, Air, Head Office and Defence Equipment and Support.

Each agent is supported by a curated, video-led knowledge bank designed for its operating environment, ensuring that guidance, examples and framing are relevant to the user's role and context.

Agents and knowledge banks are provisioned and assigned based on buyer-defined organisational scope and service requirements, rather than user self-selection.

All agents operate within the same centrally managed platform, governance model and assurance controls, ensuring consistent application of policy alignment, content standards and risk management across the service.

Service configuration enables organisations to align awareness domains, delivery priorities and reinforcement patterns to their risk profile without requiring changes to the core platform.

The service is maintained, updated and supported by the supplier, minimising operational overhead for Defence users.

7 **Onboarding and Offboarding.**

SAFER Defence is designed for rapid onboarding with minimal administrative overhead.

The service supports self-service onboarding for permanent users and sponsor-controlled onboarding for temporary or visiting users, aligned to common joiner, mover and leaver practices used across Defence environments.

Access is controlled by the buying organisation through organisation-level configuration and time-bound permissions, enabling appropriate governance of permanent and temporary access.

The service does not require integration with Defence identity systems or local IT infrastructure to begin use.

SAFER Defence can begin delivering value without requiring full organisational configuration at the point of onboarding.

The service can be introduced as a trial, pilot or phased rollout, allowing organisations to validate suitability before wider adoption.

Supplier-led onboarding support is provided to agree organisational scope, agent assignment and access controls during service initiation.

At the end of a contract, or on earlier termination, the service supports orderly offboarding, including access revocation and export of customer-accessible analytics outputs and aggregated usage data in standard formats, in line with contractual and data protection requirements.

8 Service Constraints and Dependencies.

SAFER Defence is designed to complement existing Defence training, communications and assurance activities.

The service does not replace mandated learning, formal policy dissemination or command judgement. It is intended to reinforce expected behaviours and awareness between established training and communication activities.

SAFER Defence provides guidance and awareness support but does not issue operational orders, provide live threat monitoring or replace established incident response arrangements.

Service accessible via dedicated mobile app (iOS/Android) or modern web browser on personal devices (BYOD) or MOD devices (domain whitelisted). No MODNET integration required.

The service operates independently of existing Defence learning platforms and does not require integration with them to deliver value.

SAFER Defence is designed to operate alongside existing Defence processes and does not introduce dependency on changes to established training, policy or assurance arrangements.

9 Security and Assurance Alignment.

SAFER Defence is designed to align with Defence security, safety and assurance expectations.

The service supports Defence Cyber Resilience Programmes by strengthening the human elements of awareness, behaviour and culture, which underpin effective cyber risk management.

The service aligns with Defence Safety Authority expectations by reinforcing proactive, evidence-led safety behaviours and supporting the reduction of avoidable incidents through timely awareness and behavioural reinforcement.

SAFER Defence is designed to operate in line with Defence AI assurance and governance principles, including the controlled use of AI, appropriate human oversight and alignment with organisational policy and guidance.

The service is delivered within a governed platform environment, with centrally managed content, configuration and access controls to support consistent application of assurance standards across Defence organisations.

SAFER Defence aligns to relevant Defence and wider government policy frameworks but does not claim independent certification unless explicitly stated elsewhere in the service documentation.

10 How the Service Supports Government Policy.

SAFER Defence supports UK Government and Defence policy objectives by strengthening human-layer resilience across the Defence Whole Force.

The service aligns with the Strategic Defence Review by supporting readiness, resilience and modernisation through improved awareness, judgement and behaviour in a contested and rapidly evolving threat environment.

SAFER Defence supports the Defence People Strategy by promoting digital confidence, wellbeing, competence and safer behaviours for personnel, contractors and partners operating across Defence environments.

The service aligns with the National Cyber Strategy by strengthening cyber resilience through improved human awareness and behaviour, recognising the role of people in protecting critical national infrastructure and Defence capability.

SAFER Defence supports the Whole Force Concept by enabling consistent awareness and behavioural reinforcement across military personnel, civil servants, contractors, industry partners and authorised visitors.

By providing a scalable, cross-cutting human risk awareness capability, the service supports Defence policy objectives without duplicating existing training, governance or assurance arrangements.

11 Service Features.

SAFER Defence provides the following service features.

- Dual-channel access: dedicated mobile app (iOS/Android) + web browser on personal devices (BYOD) or MOD devices (domain whitelisted). UK-hosted public cloud delivery.
- The service uses Defence-specific language, scenarios and examples aligned to operational environments and organisational context.
- A cyber awareness AI agent supports secure digital behaviours in the workplace, aligned to Defence cyber resilience expectations.
- A digital safety awareness AI agent supports understanding of home and family technology risks that may affect Defence personnel.
- A health and safety awareness AI agent supports everyday operational safety awareness and risk reduction.
- A mental wellbeing awareness AI agent supports awareness of stress, resilience and appropriate escalation routes.

- An AI awareness and misuse prevention agent supports responsible use of emerging technologies and awareness of AI-related risks.

- AI agents provide reactive guidance at the point of uncertainty or risk, supporting real-time judgement and decision-making.

- The service provides proactive learning pathways, including short Message of the Day video content to reinforce awareness over time.

- The service includes an analytics and assurance capability providing aggregated insight into engagement, awareness coverage and query trends.

- For assurance and service governance purposes, authorised Customer administrators may view selected example questions alongside associated user identifiers, such as email address. This visibility is limited, role-restricted, and intended to support organisational assurance, safeguarding, and service oversight. Full conversations and system responses are not visible to the Customer. This capability is configurable by the buying organisation and access is restricted by role and permissions.

12 **Service Benefits.**

- SAFER Defence delivers measurable benefits by strengthening human-layer resilience across Defence environments.

- The service reduces avoidable cyber, safety and behavioural incidents by providing immediate, Defence-aligned guidance at the point of uncertainty, reducing hesitation, avoidance and unreported risk.

- By delivering practical guidance in Defence-specific language and operational context, the service supports better judgement and reduces the likelihood of minor errors escalating into incidents, investigations or assurance findings.

- SAFER Defence improves operational availability by reducing preventable safety and wellbeing issues that affect personnel performance and readiness.

- The service complements mandated training by reinforcing expected behaviours where one-off courses and policy documents do not sustain awareness over time.

- Guidance and awareness content can be updated rapidly to reflect emerging threats, changes in policy and evolving risk patterns, supporting a more responsive Defence posture.

- Short, timely Message of the Day prompts build continuous awareness and reinforce behavioural expectations without adding training burden.

- The service supports consistent behaviour change at scale, contributing to improved organisational culture across the Defence Whole Force.

- SAFER Defence provides leadership with aggregated insight into awareness coverage and engagement, supporting evidence-based assurance and decision-making.

Together, these benefits support Defence readiness, resilience and cultural preparedness for increasingly digital and AI-enabled operating environments.

13 Service Differentiators.

SAFER Defence is not a traditional training product or awareness course.

The service is designed as a behavioural resilience capability that supports judgement and awareness continuously, rather than relying on periodic learning events.

Unlike conventional cyber or safety awareness solutions, SAFER Defence provides guidance at the point of need, enabling users to access relevant, Defence-aligned information when real uncertainty or risk arises.

The service uses continuous reinforcement, including short prompts and Message of the Day content, to sustain awareness and influence behaviour over time, rather than assuming retention from one-off training.

SAFER Defence addresses human risk across multiple domains, including cyber and digital behaviour, health and safety, mental wellbeing, AI use, and home and family digital resilience, recognising the shared human factors that underpin incidents across these areas.

The service operates within a single, governed platform environment, enabling consistent behaviour support across Defence organisations while allowing context-specific delivery where required.

This approach differentiates SAFER Defence from single-domain awareness tools by providing a scalable, Defence-wide capability focused on behaviour, culture and resilience rather than compliance alone.

14 Security Standards Alignment and Compliance.

SAFER Defence is designed in line with secure-by-design and privacy-by-design principles, using controls proportionate to systems operating at OFFICIAL.

The service's identity, onboarding and access control model aligns with recognised Defence, Government and industry security expectations, without requiring MODNET integration or reliance on Defence corporate infrastructure.

Access control is based on strong identity verification, least-privilege principles, sponsor-governed temporary access and defined joiner, mover and leaver processes.

Identity, authentication, permissions and lifecycle management are fully controlled within the SAFER Defence service.

AI inference services operate outside the identity and access management domain and have no access to user credentials, permissions, or access controls.

User attribution for service operations and security is handled within the Supplier-controlled service environment, and limited identity information may be visible to authorised Customer administrators where required for assurance, safeguarding, or governance purposes.

The service is designed to align with the following standards and guidance.

- Defence Cyber Protection Partnership expectations for OFFICIAL systems, including alignment with the DCPP Cyber Security Model v4.
- Government Functional Standard GovS 007: Security.
- MOD joiner, mover and leaver policy expectations.

- National Cyber Security Centre guidance on modern authentication, including Passkeys, WebAuthn and FIDO2.
- Good practice for third-party and contractor access management.
- UK GDPR and organisational data protection principles.
- Secure-by-design software development and operational practice.

SAFER Defence is Cyber Essentials accredited and is aligned with ISO 9001 and ISO 27001 control baselines.

The service keeps audit records showing user access, account changes and administrative actions, enabling organisations to review activity and provide evidence for assurance purposes.

Further detail on how SAFER Defence meets MOD security and data protection expectations can be provided during the call-off contract process, including supporting assurance documentation where required.

15 **Data Hosting and Sovereignty.**

SAFER Defence is hosted using UK-based cloud infrastructure to support Defence and wider public-sector expectations for data residency and sovereignty.

All customer data entered into the service is stored and processed within the United Kingdom, unless otherwise agreed as part of the call-off contract.

Customers retain ownership and control of their data at all times. SAFER Defence does not assert ownership over customer data and does not sell, monetise or repurpose data for non-service purposes.

Access to customer data is restricted to authorised users within the buying organisation and authorised supplier personnel, operating under role-based access controls and least-privilege principles.

Data is protected using industry-standard security measures, including encryption in transit and at rest, in line with public-sector best practice.

Where exceptional remote access from outside the UK is required for support or maintenance, this is minimised, controlled, logged, and subject to UK-approved safeguards in accordance with UK data protection law and the Call-Off Contract.

16 **Accessibility.**

SAFER Defence is designed to be accessible to users across Defence and public-sector organisations, including individuals with varying access needs, technical confidence and learning preferences.

The service is designed to align with WCAG 2.2 AA standards. These standards inform interface layout, navigation, content presentation and interaction design across the service.

Accessibility considerations include clear navigation structures, readable typography, appropriate colour contrast and keyboard-accessible functionality where applicable. The service is designed to be compatible with commonly used assistive technologies, including screen readers.

Accessibility is further supported through in-platform guidance, including short instructional videos, contextual prompts and guided walkthroughs, providing alternative ways for users to understand tasks and content without reliance on dense written material.

Accessibility is reviewed as part of ongoing service development, with issues identified through testing and user feedback addressed through the service's managed update process.

This approach supports the Customer's obligations under the Equality Act 2010 and wider public-sector accessibility expectations.

17 Service Targets, Levels and Support.

SAFER Defence is operated as a managed cloud service with defined service targets, support arrangements and recovery objectives. Support levels align with G-Cloud service desk requirements: Standard support via email/web portal; enhanced support (24x7 critical incidents) available via call-off schedule. These describe the intended operating level of the service and should be read alongside the applicable G-Cloud Call-Off Contract and service schedules.

17.1 Service availability.

The service is designed to deliver high availability appropriate to a Defence and public-sector SaaS capability. Target service availability is 99.5 percent on a monthly basis, measured across both UK business hours and 24x7 operation.

Planned maintenance is scheduled, where possible, outside UK business hours and is communicated in advance where user impact is anticipated. Downtime caused by customer networks, third-party connectivity or force majeure events is excluded from availability calculations.

17.2 Support and incident management.

User support is available through multiple channels, including in-platform support features and direct assistance, with coverage appropriate to operational use, including outside standard UK business hours where required.

Incidents and support requests are prioritised based on impact and urgency, with defined response targets for critical, high, medium and low-severity issues. Security-related incidents are handled in accordance with established incident management and escalation procedures.

17.3 Service recovery.

The service is supported by defined recovery objectives to restore availability and protect data integrity following service disruption. Recovery targets are proportionate to the service's role and will be defined within the Call-Off Contract.

17.4 Assisted use and continuous improvement.

SAFER Defence includes extensive in-platform guidance and assisted use features to reduce reliance on reactive support. Support interactions and user feedback are reviewed to identify recurring issues, usability improvements and emerging requirements, informing ongoing service improvement.

17.5 Business Continuity and Disaster Recovery.

SAFER Defence is supported by business continuity and disaster recovery arrangements aligned with the capabilities of the underlying cloud hosting environment. These arrangements are designed to restore service availability following disruptive events, maintain the integrity of customer data, and minimise prolonged loss of access. Continuity and recovery processes are reviewed periodically to ensure continued suitability.

18 Maintenance and Updates.

SAFER Defence is delivered as a continuously maintained software-as-a-service platform.

The service follows a managed update approach, under which improvements, fixes and enhancements are introduced through controlled releases rather than ad hoc changes.

Updates may include usability improvements, performance enhancements, security updates and refinements required to reflect changes in guidance, policy or the operating environment.

Routine updates are designed to preserve existing configuration and data and are deployed without disruption to customer use wherever possible.

Where planned maintenance is required, it is scheduled to minimise user impact and, where appropriate, communicated in advance.

This approach ensures that SAFER Defence remains current, secure and aligned with public-sector expectations, while maintaining service stability and continuity for users.

19 Exit and Data Retention.

SAFER Defence is designed to support straightforward, transparent and low-friction exit arrangements.

At all times, data entered into the service remains the property of the Customer. Selected example questions may be visible to authorised Customer administrators alongside user identifiers, but this does not provide access to full conversational histories or system responses.

SAFER Defence does not assert ownership over Customer Data and does not restrict the Customer's ability to access or retrieve Customer Data made available through the Service in accordance with the Call-Off Contract and these Terms.

Individual user interactions with SAFER Defence AI agents are private to the user in the sense that full conversations and responses are not accessible to the Customer.

Authorised Customer administrators may have limited visibility of selected example questions and associated user identifiers for assurance, safeguarding, or governance purposes, as configured by the buying organisation.

Customer-accessible analytical data is otherwise limited to aggregated usage information, engagement levels, and trend data.

At the end of a contract, or on earlier termination, Customers are able to export their data held within the service in standard, non-proprietary formats suitable for retention, assurance or transition to an alternative system.

Following confirmation that data export has been completed, customer data is securely deleted from the service in line with contractual obligations and applicable data protection requirements.

No exit fees are applied in relation to data export, data deletion or service termination.

20 Commercial Model.

SAFER Defence is provided under the G-Cloud 15 framework on a subscription basis.

All support, onboarding, delivery, and exit terms are governed by the G-Cloud 15 Call-Off Contract and service schedules, with these Terms applying only to the extent they do not conflict with the Call-Off Contract or its Schedules.

Pricing is published in the associated G-Cloud Pricing Document and is transparent and predictable. Charges are structured to allow Customers to scale usage proportionately in line with organisational size, scope and operational need.

The subscription includes access to the SAFER Defence service, routine platform updates, maintenance and standard support, as defined in the applicable Call-Off Contract.

There are no mandatory onboarding fees and no additional charges for routine updates or maintenance.

Contract duration, payment arrangements, renewal terms and any optional services are governed by the G-Cloud Call-Off Contract and associated schedules.