Ministry of Defence

JSP 822
Defence Direction and Guidance for Training and Education

Volume 6: Technology Enhanced Learning

Preface

How to use this Volume

1. JSP 822, Volume 6 sets out Defence Policy Direction and Guidance on Technology Enhanced Learning [1]. The volume contains the majority of Defence Learning and Development policies for Technology Enhanced Learning; where Defence policy sits outside of Volume 6, it is clearly referenced throughout the volume, and in the Coherence section at Para 5 of Volume 1.

2. The volume is made up of Direction and Guidance:

   a. **Policy Directives** which provides the Direction that must be followed in accordance with statute or policy mandated by Defence or on Defence by Central Government.

   b. **Policy Guidance** which provides the Guidance and best practice that will assist the user to comply with the Directives.

3. The volume employs '**must**', '**should**' and '**could**' language as follows:

   a. **Must**: indicates that the policy direction is a legal or key policy requirement and is **mandatory**.

   b. **Should**: indicates the policy guidance is a **recommendation**. Although not compulsory, if a decision is made that any part of this policy cannot be complied with, then the Senior Responsible Owner who is ultimately responsible for that decision must thereby own and manage the inherent risks that arises.

   c. **Could**: indicates that the policy guidance is good practice and encouraged.

4. JSP 822 is the authoritative policy that directs and guides Defence people to ensure that training in Defence is appropriate, efficient, effective and, most importantly, safe. Organisations across Defence have their own policy documents which local policy teams populate and manage, based on their interpretation of the policy contained within JSP 822.

Users should consult those policies and policy teams, within their organisation prior to JSP 822 and the TSLD Training Policy Team that manages JSP 822.

[1] Note that Organisational Learning is captured under the Defence Organisational Learning Structure (DOLS) Framework owned by Joint Warfare in STRATCOM and is not within the scope of JSP 822. The Pan Defence Skills Framework (PDSF) currently sits in Ch 4 of JSP 755

Contents

1 The Defence Learning Framework (DLF)

1. The DLF develops the Defence People Strategy's direction to maximise the talent of Defence People, providing a high-level framework encompassing the span of Defence individual and collective learning. The DLF provides key principles across ten component areas, covering all aspects of the Defence Learning Ecosystem. Detailed information on the DLF can be found in Volume 1.

Vision: Defence enables Joint Operational excellence through high quality learning that maximises the use of all the talent available to Defence.									
Mission: To enable the competent, efficient and effective delivery of UK Defence Strategic Objectives by FE@R through the provision of high quality, timely and relevant learning to Defence People.									
Key Components of Defence Learning									
Learning Governance: Effective governance structures exist with defined responsibilities and robust H2A mechanisms.	**Learning Design:** The DSAT QMS and DSAT policy and processes are applied effectively to all Defence Learning.	**Learning Delivery:** Modern, flexible learning delivery methods are employed to meet Defence and learner needs.	**Learning Environment:** Modern learning environments and technologies engage the learner in achieving high quality learning outcomes.	**Learning Culture:** A positive, proactive approach to Through Life Development (TLD) pan-Defence is embedded across the workforce	**Individual Skills Development (Professional):** Identification, acquisition and recording of Defence Professional Skills is enabled & embedded pan-Defence.	**Individual Skills Development (Personal):** Defence people are encouraged and enabled to attain personal Skills that maximise their talent (KSE-B)	**Collective Skills Development:** Deliberate and targeted learning occurs that develops team effectiveness and operational capability.	**Partnerships:** Strong strategic, operational and tactical partnerships are nurtured to maximise Defence Learning outcomes and benefits.	**Learning Futures:** Research, experimentation and innovation drives continuous improvement in Defence Learning.
Principles of Defence Learning									
1. Effective structures and responsibilities are implemented. 2. Functional and Capability Sponsors are involved from the outset. 3. Learning Requirements are clearly articulated. 4. Continuous improvement is driven across Defence Learning. 5. Risk is managed, and resource prioritised to maximise Defence Learning outcomes. 6. Robust H2A mechanisms provide assurance at all levels of Defence Learning.	1. Learning meets documented requirements and supports the attainment of Skills. 2. DSAT Analysis, Design & Evaluation functions are implemented. 3. Design staff have the necessary Skills to maximise the efficacy of learning interventions. 4. Interventions are modularised by default and access maximised. 5. Existing content is reused / repurposed to reduce duplication and maximise usage. 6. Capability development addresses the Training DLoD coherently and in a timely manner	1. Evidence-based methods are employed to achieve learning outcomes. 2. Experiential Learning is integrated into the workplace. 3. A Blended Learning approach is adopted wherever relevant. 4. Learning diagnostics are employed to establish WF Skills and enable a "fixed mastery, variable time" approach. 5. Delivery staff have the necessary Skills to support learners to achieve enhanced learning outcomes. 6. Learners have the necessary learning and technology Skills to achieve enhanced learning outcomes.	1. Physical and virtual learning environments are safe, engaging and accessible high-quality places. 2. Learning technology capabilities are developed iteratively in an 'evergreen' approach. 3. A pan-Defence Learning Management and Delivery System: a. Provides coherent Information to enable evidence-based investment and policy decisions. b. Enables coherent and efficient Governance, Design, Delivery, Assessment and Evaluation. c. Enables immersive learning.	1. Positive attitudes to learning are demonstrated at all levels of Defence. 2. WF have the opportunity and support to undertake purposeful learning. 3. Learning achievement is rewarded and recognised. 4. Informal learning opportunities are encouraged, supported and exploited. 5. Duty of care and trainee welfare is prioritised in all learning environments. 6. Learning design & delivery account for the learning needs of a neuro-diverse workforce.	1. WF Skills are captured and recorded in a single pan-Defence repository. 2. Defence Skills records are utilised to: a. Exploit workforce talents to meet Defence Strategic Objectives. b. Enable professional development and career progression. 3. Professional Skills Development is based on clear learning outcomes and recognition of accredited / prior qualifications & learning.	1. A personalised learning pathway, a Skills Passport, and coaching and mentoring provision is available for all. 2. Individuals 'own' and 'value' their personal learning journey, supported with access to learning, qualifications, time and resources. 3. Individuals are encouraged to develop Skills and gain qualifications to prepare them for life beyond Defence.	1. Collective Training is focussed on the development of teamwork capabilities. 2. Methods and tools are used to accurately measure and assess teamwork capabilities and skills. 3. Identify, measure and evaluate collective team & task outcomes at all levels. 4. A full mix of Live, Synthetic and Blended methods are used to provide Collective Training interventions.	1. Collaboration with PAGs, UK Defence Allies and external organisations is harnessed to improve learning outcomes for the benefit of Defence. 2. Collaboration with DfE influences Government learning policy for the benefit of Defence and its WF. 3. Collaboration with partner organisations enables the delivery of apprenticeships, professional accreditation and intellectual development programmes. 4. Outsourced Defence Learning contracts are managed and assured effectively.	1. Lesson exploitation and horizon scanning identifies opportunities and priorities for learning research. 2. Research work in partnership with DST, DSTL and contracted partners is: a. based on agreed requirements; b. supported and exploited into practice. 3. Opportunities to experiment and innovate are created, and outcomes are transferred into BaU where appropriate.

2 Defence Direction for Technology Enhanced Learning (TEL)

Policy Sponsor: TSLD, CDP.

The TEL Direction contained within this Chapter provides Defence Policy for all Defence & Contractor personnel involved in developing, procuring or integrating TEL provision across Defence. TEL is part of the wider digitisation of Defence[2] and, specifically, across the Defence People Area. Specific direction on the Defence Learning Environment (DLE) and the Training and Financial Management Information System (TAFMIS) follows in Chapters 3 & 4. The TEL Ruleset is set out in Chapter 5.

2.1 Introduction

1. **Definition of TEL**. TEL is defined as '*Technology that improves the design and delivery of training in order to enhance learners' experience'* and is commonly taken to mean *'Information Technology'*.

2. **Defence TEL.** Defence TEL ranges from Training Management Information Systems (TMIS') to Virtual Learning Environments (VLEs) to Modelling & Simulation (M&S) Environments[3], encompassing a wide range of TEL tools within these broad capabilities. There are currently multiple TEL systems and environments across Defence but the endorsed direction of travel is to ensure common usage of approved, integrated TEL capabilities across as much of Defence as possible, leading to a coherent and connected Defence TEL landscape and a corresponding reduction in the number of TEL systems and environments employed.

3. **Defence TEL Role.** TEL is a key enabler for Defence Individual & Collective Training. TEL enables the Defence Systems Approach to Training (DSAT) through all elements of Analysis, Design, Delivery and Assurance, with a particular emphasis on enabling the delivery of Defence Learning (Training & Education).

4. **Outcomes.** Defence TEL is a key enabler in delivering the Defence Learning Framework (DLF) vision of 'enabling Joint Operational excellence through high quality learning that maximise the use of all the talent available to Defence'. This in turn delivers the key Defence People Strategy aim of 'Maximising Talent' of Defence People in support of delivering Defence Strategic outcomes.

5. **Defence Learning Framework (DLF).** This provides the overarching Defence Learning Strategy and the context within which TEL must be employed to support Defence. TEL has a key role to play in enabling achievement of all the DLF components. In particular, the development and employment of TEL is critical in realising the 'Learning Environment' component: 'Modern Learning Environments and technologies engage the learner in achieving high quality learning outcomes'.[4]

---

[2] As set out in the Defence Digital Strategy.

[3] Inclusive of gaming, virtual reality (VR), augmented reality (AR) and mixed reality (MR) environments, collectively referred to as XR.

[4] Prior to disbandment, the DEFAC DTEL Team developed a Defence TEL Strategy in support of the Defence Learning Framework (DLF) – in turn part of the Defence Learning TOM – and a TEL Capability Maturity Model; both can be found for reference on the TEL Knowledge Hub.

6. **Purpose.** This JSP 822 TEL Volume principally provides Defence Direction & Guidance on TEL in general and TAFMIS & DLE specifically plus their future replacements through the DLMC Programme. Direction and Guidance on Command-specific TEL is provided by each Command where relevant through appropriate TEL policy documents and Command TEL 'Hubs'.

7. **Defence TEL Knowledge Hub.**[5] The TEL Knowledge Hub[6] on the DLE is a repository for current guidance and information on TEL good practice. This provides a hub for Command TEL Hubs to link into and enables Defence TEL designers, trainers and managers to explore and exploit TEL opportunities in a collaborative manner, improving TEL application and usage across Defence.

2.2 Defence TEL Primary Systems

8. **Defence TEL TMIS & VLE**. TAFMIS is Defence's current approved TMIS. The DLE is Defence's current approved VLE. TAFMIS and DLE are currently owned by the DLMC Programme on behalf of Defence and delivered respectively by Army Digital Services (ADS) and the DLE Service Delivery Team (DLE SDT), Digital Foundry, Defence Digital.

9. **Use of Defence Primary TEL Systems.** The following direction applies to the use of TAFMIS and the DLE pan-Defence:

a. TAFMIS must be used as the Defence mandated TMIS wherever possible. This will support pan-Defence transition to DLMC replacement services for TAFMIS provision in due course.

b. The DLE[7] must be used for all Learning (Training & Education) requiring the use of a VLE to enable the T-DLOD through online and blended learning.[8]

10. **Defence TEL M&S.** M&S environments & tools are directed by the Defence Modelling & Simulation Office (DMSO) in StratCom and designed in accordance with policy and rules set out in JSP 939.

2.3 Defence Learning Management Capability (DLMC) Programme

11. **Vision, Intent & Strategic Objectives.** The DLMC Programme Mandate sets out the vision, intent and strategic objectives as follows:

a. Vision: "Defence people, fully enabled by their digital learning and management services, shaping a sustainable workforce and maximising the use of Defence talent in support of Operational Capability".

[5] The TEL Knowledge Hub is run by SO2 TEL R&D, CEDERA, DEFAC on behalf of Defence.
[6] For systems where the link does not work from this document copy this link to the browser:
DLE: https://www.dle.mod.uk/course/view.php?id=14579
MODNET: https://modgovuk.sharepoint.com/teams/17799/DTEL/SitePages/Home.aspx
[7] The DLMC Programme has endorsed the use of Moodle as the VLE software for future DLE.
[8] Note that an anonymised instance of the DLE, referred to as the Cyber VLE, runs in parallel to the DLE for those Defence personnel requiring anonymised access to learning.

b. Intent: Future DLMC services will modernise the services provided by TAFMIS and DLE legacy systems through the delivery of integrated TMIS and VLE digital services.

c. Strategic Objectives: DLMC is to deliver digital learning services through a modernised, flexible, pan-Defence learning management and delivery capability that will:

1) Provide modern, accessible, engaging and evergreen learning management and delivery services that meet the Defence workforce's expectations, improve motivation to engage with learning and enhance their learning experiences, enabling our people to plan, access, achieve and record the learning required in support of their personal career goals.

2) Enable a cohesive, effective, resource-efficient Defence Learning (Training & Education) System that meets the learning and professional development needs of the Defence Workforce.

3) Support the delivery of the Defence People Strategy.

4) Provide coherent, timely pan-Defence learning information that enables improved Defence decision-making on workforce planning and structures, workforce exploitation and development, and investment in learning.

5) Enable the Defence Skills Framework by capturing and tracking relevant workforce skills.

6) Enable governance and assurance of Defence Learning (Training and Education), and assurance of compliance with policy frameworks.

7) Resulting in identification and development of workforce skills that enables optimal exploitation of the Defence Workforce to deliver future operational requirements

12. **Responsibilities.** DLMC is a programme in the Defence People Portfolio, sponsored by Defence People and delivered by the DLMC Programme Team located in Army Command. Key Responsibilities are:

a. Functional Sponsor: ACDS People Capability, Defence People Team.

b. Sponsoring Group: People Leadership Team, a 3* chaired Forum with 2* reps from all Commands).

c. Senior Responsible Officer (SRO): Hd IX, Army DINFO.

d. Programme Board: 1* Forum with reps from all Commands, chaired by SRO.

e. Business Change Managers Forum: OF5 Forum chaired by AH Trg Pol/Assurance TSLD.

f. Lead Users Forum: A desk level forum representing the business requirements of all commands, chaired by SO1 Trg Cap TSLD as the Defence Lead User.

13. **Ownership.** The DLMC Programme owns and is responsible for the current TAFMIS and DLE services. The Programme Team work in conjunction with a range of stakeholders, in particular the TAFMIS Delivery Team in Army Digital Services (ADS) and the DLE SDT in Digital Foundry, Defence Digital, to deliver TAFMIS and DLE services[9]. The DLMC Programme is responsible for delivering future DLMC services to replace and/or improve existing TAFMIS and DLE services over the course of the Programme lifetime; transition of future DLMC services to a permanent delivery owner is a key element of the DLMC Programme.

14. **DLMC Information & POCs.** Information on DLMC progress & relevant POCs can be found on the DLMC Comms Hub on MODNET. There is also a DLMC User Group Network DLMC User Group Network (CoI) on the DLE.

2.4 TEL Procurement

15. All procurement of TEL across Defence must comply with Government Digital Services (GDS) regulations and follow the TEL Ruleset (see Ch.5), based on the GDS Technology Code of Practice). This will ensure robust analysis of the TEL requirement, minimising duplication of existing TEL and providing sufficient evidence for business cases to be approved by the Cabinet Office or delegated approvals authority. Detailed rules for M&S TEL procurement are set out in JSP 939.

2.5 TEL Coherence and Collaboration

16. **DLMC.** The DLMC Programme provides a cohering function for Defence TMIS and VLE provision through the design and delivery of future DLMC services. The Programme Team also run a change control process for improvements to existing DLMC (TAFMIS & DLE) services[10].

17. **Defence TEL (DTEL) Working Group (WG).** The DTEL WG (co-ordinated and chaired by SO2 TEL R&D, CEDERA, DEFAC) acts as a Defence hub to share and collaborate on TEL challenges, initiatives and programmes. All TLBs are represented on the DTEL WG. See the DTEL WG DLE site and DTEL WG Teams Channel.

18. **UK MOD ADL WG.** The UK MOD ADL WG is a voluntary WG attended by motivated reps from across Defence to discuss and promote resolution of technical TEL issues across Defence and to engage with NATO ADL initiatives and WGs, including the development of TEL-related STANAGs. See the UK MOD ADL WG SharePoint site for further details.

19. **NATO Training Group Advanced Distributed Learning (ADL) Programme.** The ADL Programme is a US-led NATO TEL programme developing NATO TEL Policy and Guidance. *(Link to Site and Handbook to follow)*

20. **DLE Training Support Working Group (Trg Sp WG).** The DLE Trg Sp WG provides a forum for the management and review of DLE Training requirement setting, design,

[9] Note that an anonymised instance of the DLE, referred to as the Cyber VLE, has been launched and runs in parallel to the DLE for those Defence personnel requiring anonymised access to learning. Ownership nominally resides with the DLMC Programme but funding comes from Defence Cyber.
[10] TAFMIS and DLE Changes are managed, prioritised, designed, delivered and assured by the TAFMIS Manasgement of Change (MOC) and DLE Service Delivery Team (SDT) respectively with direction from the DLMC CCB as required.

delivery and assurance. The DLE TWG (co-ordinated by DCTS) informs and supports the DLE CEB (co-ordinated by DCTS).

21. **The Defence People Function Coherence Group.** Led by the Defence People DDaT Team, it provides a cohering mechanism for exchanging knowledge on all Defence HR and Learning/Training Digital initiatives to enable sharing of good practice and collaboration.

22. **TACK Model.** The Technological, Andragogical and Content Knowledge Model provides a mechanism for cohering TEL requirements and knowledge to support the TLBs and TEL WGs in TEL collaboration & exploitation. The TACK Model is available on the TEL Knowledge Hub on the DLE.

23. **TEL Integration.** TEL Integration at Defence level is driven through the DLMC Programme, the DTEL WG and the UK MOD ADL WG. Commands are responsible for engaging with the Defence TEL Integration mechanisms and developing their own TEL Integration mechanisms as appropriate in line with Defence TEL policy, including the TEL Ruleset (see Ch 5).

2.6 TEL Governance & Assurance

24. **Defence TMIS & VLE.** Currently TAFMIS and the DLE respectively, these are governed and assured through the DLMC Programme Boards, specifically:

a. The DLMC Service Delivery Board.

b. The DLMC Programme Working Group.

c. The DLMC Change Control Board.

25. **Defence Customer Consultation.** The Defence Customer is consulted on TAFMIS and DLE provision through:

a. The DLMC Programme Board (1*).

b. The DLMC Business Change Managers Forum (OF5).

c. The DLMC Lead Users Forum (LUF).

d. In addition to the DLMC Change Control Board.

26. **Defence M&S.** Defence M&S is governed and assured through DMSO Boards and Working Groups.

27. **Customer Executive Boards (CEBs).** As a key enabler (methods and media) to learning (training & education) design and delivery, the use of TEL is to be considered by CEB training governance and assurance functions.

28. **Working Groups (WGs).** As set out at Section 2.5 Paras 16 – 21. Ch 2 Para 27.

3 Defence Direction for the Defence Learning Environment (DLE)

Policy Sponsor: TSLD, CDP

The DLE is Defence's primary and mandated Virtual Learning Environment (VLE) which currently utilises four systems: Moodle (Learning Management System); Alfresco (Content Repository); Learning Locker (Learning Record Store); and Mahara (ePortfolio). These systems are continuously developed to improve user experience and increase the effectiveness of online and blended learning within Defence.

3.1 DLE Governance

1. **DLE Governance**. DLE Governance is set out in JSP 822 Vol 6 Chapter 2 Section 2.6.

3.2 DLE Roles & Responsibilities/Permission Sets

2. The DLE has a number of roles that require training and additional system permissions. Below is a brief description of each role[11]. For full role responsibilities see the DLE Knowledge Hub.

    a. **Defence Administrators**. Provide overarching support and guidance on the system, supporting Category Managers to maintain appropriate working practices within their School.

    b. **Category Managers**. Manage the TLB presence on the DLE. Provide governance and responsible for managing and maintaining their TLB structures, including but not limited to ensuring that their environment holds only official information.[12]

    c. **Sub-Category Managers**. Manage the Sub-Category presence on the DLE. Provide communication and support of endorsed policy while providing governance for courses within their remit.

    d. **Course Designers**. Design and develop courses on the DLE. Provide advanced course design for learning iterations on the DLE within their remit. All courses delivered on the DLE must be designed by a DLE Course Designer.

    e. **Course Owners**. Own the course content and are the single point of contact for any queries relating to course content and functionality.

    f. **Administrators**. Administer courses hosted on the DLE, including but not limited to managing DLE course instances and assigning permissions at course-level.

[11] These role descriptions will be reviewed and updated as required as part of the DLE Training Review currently taking place. Note the additional roles of Learning Plan Supervisor & Viewer will be added in the V7 Update.

[12] There is also a Deputy Category Manager role to provide support and cover for the Category Manager.

g. **Trainer**[13]. Deliver and support training hosted on the DLE, including but not limited to creating course content. This will also facilitate learner use of the DLE. Sub-categories of the Trainer role are:

(1) **Non-Editing Trainers**[14]. Use the DLE to deliver and support training but have no editing rights to change course content.

(2) **Assessors**. Manage, maintain and administer assessments within the DLE ensuring that requirements for aspects such as copyright, plagiarism and security classification are met. Note: it is anticipated that all Trainers will become accredited assessors in due course.

(3) **Turnitin**. A new DLE role has been created specifically to manage plagiarism detection tools (Turnitin) and check assignments. There will be two types of users that will hold the Turnitin DLE role:

(a) Turnitin account manager, responsible for unit management of Turnitin.

(b) Trainers or assessors who will create Turnitin assignments and check outcomes.

3.3 Application of DSAT to DLE Learning Content & Delivery

1. All learning instances and content hosted on / delivered via the DLE – whether delivered online or as part of a blended learning delivery - must be governed and managed as part of an MTS in accordance with DSAT Direction & Guidance in JSP 822.

3.4 DLE Quality Rubric

2. The DLE Quality Rubric is located on the DLE Knowledge Hub. The purpose of the DLE Quality Rubric is to provide an assurance framework for DLE Learning Design & Delivery.

3.5 DLE Assurance

4. Formal training that is delivered online should be subject to formal training quality assurance processes in the same way as any other formal training and education activity. The DLE Quality Rubric should be used as part of the DSAT 1st and 2nd party audit process[15] for any course that uses online learning or has identified digital Work Based Training. This will help improve the quality of courses and to identify key areas for improvement. The DLE Quality Rubric involves scoring courses against a range of criteria and any Red scores should form part of a non-compliance task list for each course.

[13] Trainers must complete the DLERFT Foundation Module. This is required to be able to use the DLE effectively, updating Cse content when required and building an awareness of DLE capability.
[14] This role is required by auditors to complete their tasks.
[15] As set out in JSP 822.

5. It is recommended that an additional Topic is created within each course and that the DLE Quality Rubric and its action plan are stored there, where it is visible to students.

3.6 DLE Accounts (DLE User)

6. All Defence personnel and supporting contractors are entitled to access learning available via the DLE.[16] Other personnel requiring DLE access include UK MOD recruiting candidates with a training start date, international students, exchange personnel and personnel from other Government departments. To ensure these varied needs can be met whilst also maintaining appropriate security and access controls, three types of account have been created:

a. **Full Account**. These accounts can be created by all MOD staff either with a MOD email address or Service Number by logging into www.defencegateway.mod.uk and creating a DLE account.

b. **Full Sponsored Account**. These are requested from the DLE team using the Defence Gateway Application form. This grants full access and rights to the DLE, including self-enrolment onto courses, for a maximum of two years. Accounts of this nature need a sponsor of OF3/C2 or above.

c. **Limited Access Student (LAS)**. These are requested from the DLE team using the Defence Gateway Application form. This grants limited (read only) access and no enrolment rights onto courses. Users with this account must be manually enrolled onto courses by the course owners.

7. All queries on DLE accounts should be submitted through the Service Centre 1st Line Helpdesk (DLE) in the first instance.

3.7 DLE Training

8. The DLE provides a Virtual Learning Environment (VLE) for the delivery of online and blended learning. To use the DLE effectively, and to gain DLE permissions, DLE Training must be completed.

9. DLE Training is currently constructed as follows:

a. DLE User Training: A DLE User Module provided as an optional, self-paced (& self-enrol) online learning course on the DLE.

b. DLE Role Functionality Training (DLERFT): This provides a learning pathway of five self-paced (& self-enrol) online learning courses tied to DLE roles and permissions which must be completed prior to the related DLE permissions being authorised by Category Managers/Sub-Category Managers permissions on successful completion. The courses and attached permissions are set out in at the table on the DLERFT page.

[16] In order to obtain a DLE account, personnel must have a Defence Gateway account.

c. DLE Digital Design & Delivery Training: Currently provided through the Designing Online Learning Course (DOLC), a 2 day F2F or virtual online course at/by DCTS, DEFAC to enable acquisition of improved DLE Learning Design skills.

d. DLE Elective Training:

i. DLE Turnitin Training is provided as a self-paced online learning course for those needing to gain permission to use the Turnitin plugin.

ii. DLE Additional Functionality modules are available on the DLE as optional self-paced (& self-enrol) online learning modules to enhance DLE skills.

3.8 DLE Content Sharing

10. All common/reusable DLE content should be stored in Alfresco within the DLE to enable reuse by organisations across Defence and hence prevent repetition and duplication of effort.

11. To enable common/reusable content to be found for re-use, learning designers must tag the learning content by subject using the DTEL Taxonomy.

12. Further details on the use of Alfresco and tagging through use of the DTEL Taxonomy can be found on the TEL Knowledge Hub DLE Policy & Guidance Book at Alfresco Content Storage and Moodle Content Tagging.

13. Where appropriate and relevant, DLE content should be made available to NATO Allies. This may require a SCORM version of the DLE content to be created to enable sharing with NATO Allies (as set out in STANAG 2591). NATO learning content is available *here*. *(link required).*

3.9 DLE Naming Conventions / Learning Catalogue

14. Every effort should be made to allow learners to identify the type of course being delivered from its name. To help improve the utility of the DLE Search Engine and future implementation of a DLE Learning catalogue, all DLE courses are required to be given (by the Learning Designer) a long and short course name based on the following structure:

a. Course Code: Use one of the abbreviations below:

i. OT: Formal Training delivered online.

ii. PC: Pre-course learning.

iii. IP: Information Point.

iv. CL: Collaborative Learning Environment

v. CT: Collective Training.

b. Course Name: Full and Abbreviated.

c. TLB:

i. N – Navy.

ii. G – Army

iii. A – RAF

iv. J – Joint

d. JPA Number – For mandatory courses only which are logged on JPA as a competence. Only required for the long name.

15. An example is as follows:

a. Short Name: PC S&A A

b. Long Name: PC Skill at Arms RAF

16. Further detail on the DLE course naming convention can be found at DLE Naming Convention.

3.10 Evolving DLE Capability and Function

17. The DLE is a continually evolving system with increasing capability and a wide variety of potential uses. Further detail on capability developments and guidance on how to use the DLE can be found in the TEL Knowledge Hub and in particular the DLE Policy and Guidance Book. The DTEL WG, Command TEL WGs and DLE SDT DLE WGs provide forums in which DLE capabilities and uses can be discussed and expertise shared.

4 Defence Direction for the Training and Financial Management Information System (TAFMIS)

Policy Sponsor: TSLD, CDP

TAFMIS is Defence's primary and mandated Training Management Information System, accessible via MODNET and available pan-Defence. TAFMIS is a DLMC Live Service. TAFMIS is continuously developed to improve user experience and increase the effectiveness of Training Analysis, Design, Delivery and Assurance within Defence. This Direction & Guidance applies to all Royal Navy, Army, Royal Air Force and Joint Individual Training Providers throughout Defence that use TAFMIS. *It also covers JPA OLM for those providers not provided with access to TAFMIS*.

4.1 TAFMIS Scope

1. It is mandated that all organisations provided with TAFMIS are to use TAFMIS to manage the individual training, events, processes and resources of people engaged with Phase 1, Phase 2 and Phase 3 training. [17] This is essential to ensure a consistent approach to DSAT and to provide coherent and complete management information across Defence.

2. All other individual training organisations must instead use JPA OLM for course bookings, the recording of competences and completing training history.

3. TAFMIS directly enables the application of the DSAT process for Defence Training & Education. Details on TAFMIS services can be found in the briefing documents at TAFMIS PORTAL MOC Team TAFMIS Briefings and at Section 4.9 below.

4. The course naming conventions laid down in JSP 794 are to be used, where possible, on both TAFMIS and JPA OLM. JPA contains the master list of competences for both systems – new competences cannot be created in TAFMIS. The protocols for change are laid down in JSP 794.

5. Organisations seeking to use TAFMIS as the Defence-mandated TMIS must request access via the change process; see the TAFMIS Portal for details[18].

4.2 TAFMIS Governance

6. **TAFMIS Governance**. TAFMIS Governance is set out in JSP 822 Vol 6 Chapter 2 Section 2.6

[17] For the Army, Phase 1 is termed Basic Training (BT), Phase 2 is termed Initial Trade Training (ITT) and Phase 3 is termed Subsequent Trade Training (STT).
[18] And Army Information Front Door ; enter 'TAFMIS' in the search box and this will bring up the TAFMIS RFC forms.

4.3 TAFMIS Roles and Responsibilities

7. **Service Delivery.** The Army is the Lead Service for TAFMIS delivery. The TAFMIS service is delivered by Army Digital Services (ADS) based in Army HQ, Andover. ADS are responsible for delivering the capability together with its full-service management, including a dedicated helpdesk. Incidents should be raised via the Service Centre which are then passed to the TAFMIS Application Support team to resolve. Change requests should be submitted via the TAFMIS change process[19].

8. **TAFMIS Managers**. All Defence training sites identified for, or supplied with, TAFMIS are to appoint a TAFMIS Manager. The TAFMIS Manager will be the single point of contact for that site and are to follow the ToRs for TAFMIS managers. Initial nomination of and any change to a site's TAFMIS Manager is to be notified to the appropriate Headquarters. Service Headquarters should advise ARITC of all changes to TAFMIS Managers.

9. **Key TAFMIS POCs.** These are listed on the TAFMIS SharePoint Site.

4.4 TAFMIS Access

10. **TAFMIS Infrastructure Requirement**. TAFMIS is designed to be accessed from MODNET desktops and laptops across an RLI-connected infrastructure. Where MODNET is not available, RLI-connected infrastructure is needed at the MODNET desktop build standard. Failure to do this may affect the performance of the TAFMIS software.

11. **TAFMIS Accounts**. TAFMIS Accounts are arranged via TAFMIS Site Managers. TAFMIS users are responsible for managing their accounts through the registration and use of the AHE Self Service Password Manager tool.

4.5 TAFMIS Training

12. **TAFMIS Training**. Users must be TAFMIS trained to a level appropriate for their role. Users may be granted access to TAFMIS prior to attending TAFMIS training, but they are required to complete the relevant courses within 3 months of appointment. If a user fails to complete training within the prescribed time, their supervising TAFMIS Manager will be notified that system access will be withdrawn from that user until such training is completed successfully. Descriptions, dates and booking procedures for TAFMIS courses can be obtained from TAFMIS Managers. Details on TAFMIS training are available via the TAFMIS Training Portal.

4.6 TAFMIS Continuous Improvement

13. **TAFMIS Change Management**. TAFMIS Change Management is authorised through the DLMC Change Control Board and managed by the TAFMIS Management of Change (MoC) Team.

[19] Go to Army Information Front Door and enter 'TAFMIS' in the search box; the will bring up the TAFMIS RFC forms which should be submitted by the local TAFMIS Manager.

14. **TAFMIS COI.** Each module within TAFMIS should have a COI to share good practice and develop coherent change requests. These will operate on a mix of SharePoint/MOSS and face-to-face meetings, facilitated by ARITC and supported by the TAFMIS MOC Team.

4.7 TAFMIS Support

15. **Service Centre**. Issues with TAFMIS should be reported to the Service Centre; where required these will be passed to the TAFMIS Helpdesk for resolution.

16. **TAFMIS Portal**. A range of supporting information for TAFMIS is available via the TAFMIS Portal.

17. **Business Intelligence Service.** The Business Intelligence Support Manager is located in HQ ARITC in the Recruiting & Training Intelligence Cell (RTIC). The role exists to exploit the information available from TAFMIS and EMIS. It provides the following services:

a. Advising on Management Information (MI) and Business Intelligence (BI) as required to support the business.

b. Advising on TAFMIS data structures and data quality issues.

c. Enhancing TAFMIS modules and advising on the implementing of data patches as required to address specific data quality issues.

d. Authorised TAFMIS Change Manager.

e. Advising on business processes associated with data quality issues.

18. **TAFMIS Standard Operating Procedures (SOPs).** To ensure that the use of TAFMIS (both process and data) is consistent across Defence Training & Education, all organisations using TAFMIS are to use the TAFMIS Workbooks and Quick Reference Guides for each of the TAFMIS modules. These are available via the TAFMIS Portal. Further detailed information and instructions on new releases to TAFMIS are also held on the TAFMIS Portal along with relevant service management forms.

4.8 TAFMIS Assurance

19. **1st & 2nd Party Audit**. Use of TAFMIS in line with TAFMIS Policy, SOPs and direction in TQMs is to be assured and reported on as part of 1st and 2nd Party Audit. Direction on the use of TAFMIS should be laid down in TRA/TDA/TP TQMs as part of the MTS.

20. **Integration with other systems.** The integration between TAFMIS and other systems means that changes to the implementation or use of one could impact on the others. Consequently, all system changes must be considered carefully and authorised by the appropriate Headquarters and, where necessary, at the Programme level.[20]

[20] The HQ/Programme must ensure that the systems requiring integration with TAFMIS comply with the recognised learning standards (see Rule 4 TEL Toolset).

21. **Data quality**. The premise of enter data once, use many times works best when accurate data entry is made in the first instance. Data quality is a measure of the condition of data based on factors such as accuracy, completeness, consistency, reliability and time-sensitivity. Increasingly, the use of data analytics to help drive business decisions has emphasised the need to be able to have a single version of a truth to enable successful recruiting and training operations. All TAFMIS users must ensure that data entered into TAFMIS is compliant with data quality standards. To save time, effort and resource, all data entry is to be conducted as soon as practical, with specific attention paid where data is added near to or on month end.

22. **Data Changes**. Training Providers are to implement a system of validating the data entered into TAFMIS systems and include this in their TQM. When instances of duplicate records, in correct service numbers and records assuming a previous state (e.g. a trainee marked back on site by TAFMIS after being marked off site, or data entered by site, which is then overwritten by TAFMIS) are identified, users are to raise a data change request using the appropriate form on the TAFMIS Portal. Further action may require the submission of a TF and sites are to follow the current guidelines laid down by the TAFMIS Service Manager.

23. **Responsibility for data quality**. Within each Service's individual training headquarters, a role is to be nominated to take overall responsibility for TAFMIS data quality. Within each Training Provider, a 'Data Champion' is to be appointed with overall responsibility for data quality. Across individual training at all levels, the active monitoring and management of data quality is to take place so that the full benefits of TAFMIS can be realised. Advice and Guidance for all data quality issues can be requested from the ARITC Business Intelligence Support Manager.

4.9 TAFMIS Modules

24. **Course and Student Administration (CA).** Essential management information is gathered by the system from CA users dealing with such areas as Course Administration, Student Administration and Trainee Tracking. These functional areas provide managers with visibility of trainees from recruitment through to assignment to the SCs equipped for operations. Consequently, this module, including the Trainee Tracking function, is to be fully implemented by Training Providers as a first priority.

25. **Training Analysis Developer (TAD).** TAD supports the DSAT analysis & design process for Training Requirement Authorities (TRAs) and (TDA) Course Design Cells (CDCs). Given the effort involved in migrating to TAD, CDCs who are not already using TAD must liaise with TRAs to prioritise the migration to TAD. TAD will automatically populate fields throughout the course folders, such that as the TRA migrates courses, the CDC will be able to access TAD course documentation. Consequently, all training units not already using TAD are to aim to use TAD in its entirety as soon as possible. It is recognised, however, that the migration of large quantities of legacy information into TAD by Training Development Teams (TDTs) and CDCs new to TAFMIS is challenging. As a result, the TAFMIS Team will be available to assist in the change process where needed.

26. **Templates (CME).** The Templates module is used to create a graphical model of how elements of the course will be run from start to finish. It allows definition of the number of lessons per day or week, time flow of lessons linked to the course calendar and examination positioning. Resource and trainer requirements and TOs can be added to individual or multiple elements. This provides information on the resources used for training,

with a forward projection of resource requirements and, potentially, costs. An important aspect of the Templates module is that it enables the capture of information necessary to improve management of resources, balancing their use to achieve greater efficiency. Templates also provide links into courses to automate InVal. As a minimum, Training Providers are to show each course in sufficient detail to support an accurate assessment of the utilisation of trainers and those key resources with a significant associated cost. The design of courses that call on several different, costly resource types for different lessons/events will need to be prioritised for production in more detail. Data input into the Templates module provides automatic inputs to other modules – for instance, it is essential to identify the 'test' elements in course templates in order to allow the Assessment and Validation modules to function.

27. **Planning and Scheduling Tools (PST).** Training Providers are to use PST. To meet the minimum requirement for use, the current year's 'schedule' must hold a programme of courses with associated start and end dates, as well as associated key resources. This enables trainee administration, InVal and trainer/resource management to be accomplished using TAFMIS. In addition, skeleton schedules must be created as far into the future as is required to support 'Trainee Tracking' assignments and 'Recruit Allocation Planning'. By fully utilising PST, Training Providers will be able to:

a. Manage resource shortfalls.
b. Find the best dates for courses based on the course template and availability of resources.
c. Schedule non-course activities.

28. **Resource management.** The resource management module identifies the requirement for resources that are required to deliver training and is to be used. Training Providers are to use TAFMIS to define those resources that are significant cost drivers or of greatest importance and utility to their own schedulers and resource managers. The Service and Joint individual training HQs are to work together to deliver standardisation of naming of resources to enable balancing and sharing of key resources across Training Groups, Commands and Services where this is sensible.

29. **Trainer management.** The trainer management module identifies the requirement for trainers that are required to deliver training and Training Providers are to enter trainer details in TAFMIS and use the facility to manage trainers. TAFMIS supports the management of trainers in relation to training and non-training activities.

30. **Course assessment.** The Course Assessment module provides the functionality to manage question banks, exams and statistics, and to create questionnaires and must be implemented. The scanning software enables the automated input of answer sheets.

31. **InVal and ExVal.** The TAFMIS module that supports InVal and ExVal is called Course Validation. InVal supports course evaluation during and at the end of courses and is usually carried out by Training Providers. ExVal is the responsibility of the TRAs. Where available to TRAs, they are to use this module. The primary purpose of ExVal is to determine the impact on performance after training activity and, therefore, the validity of the training in preparing individuals for their Role. It measures changes in the behaviour of individuals as a result of a training activity and how well the enhancement of KSA has prepared individuals for their Role. Findings from ExVal may be used by the TRA during TNA in the review of the Role PS.

4.10 TAFMIS Information Systems & Data

32. **Business Intelligence (BI)**. At the Headquarters level a BI cell[21] is needed to address corporate information needs. The requirement is to gather, collate, analyse and report management information on the performance of the recruiting and training pipeline to provide BI in order to support the commanders' decision processes. TAFMIS provides two Capabilities for the provision of management information and business intelligence:

a. **Business objects.** Business Objects is the reporting software that enables the extraction of day-to-day reports and management information from TAFMIS, which can then be published on SharePoint. Business Objects must be used to prepare all reports on training data within the scope of TAFMIS in order to:

(1) Minimise the need for duplicating and/or re-keying data.
(2) Support the Defence intent of establishing 'one version of training truth'.

Reporting protocols and needs will be promulgated by the respective Headquarters, consistent with a common approach across Defence.

b. **Enhanced Management Information System (EMIS).** The EMIS Data Warehouse is an extension to the TAFMIS Management Information capability across recruiting and training to meet the emerging need for Business Intelligence. EMIS provides stakeholders, through visibility and exploitation of data, with accurate management information to:

(1) management information in an agile manner so that decisions can be made.
(2) Enable better informed management reducing the potential for data mismanagement.
(3) Increase the effectiveness and, where possible, efficiency of the recruiting and training pipeline.

33. **SharePoint.** The output of Business Objects reports can be converted into PDF, Word or Excel documents for publication to designated SharePoint sites appropriate to the Customers for the reported information. In this way, the number of Business Objects licences can be kept to a minimum.

34. **System interfaces.** The TAFMIS module suite is an integrated design intended to support all the principal functions of training design and administration. Data entered into TAFMIS is shared amongst several systems including the Defence Recruiting System (DRS), which is planned to be replaced by the Recruiting Partnering Programme (RPP) recruiting solution and JPA. All of these systems rely on the timely and accurate input of data to ensure the underlying processes work correctly and accurate management information is available. The system interfaces have been developed to support the concept of 'enter data once, use many times'. This means that some of the data captured throughout recruitment and training is passed to JPA to be recorded on an individual's record of service, enduring throughout their entire career.

[21] The ARITC Recruiting and Training Information Cell (RTIC) provides this service on behalf of the SRO and all TAFMIS users.

35. **Data exchange.** Data is exchanged between the TAFMIS modules in a number of ways:

a. **TAD.** TAD provides a mechanism for creating, storing, amending and linking the data required for course analysis and design. TAD supports the DSAT process from organising the results of a RA through to developing a full LSpec. At the relevant stages, approvals and authorisations are available to support the exchange of information between TRAs, TDAs and Course Design Cells. Data from TAD is used in Templates.

b. **Templates.** Templates provide functionality to design a course and define the duration, timing, content, resource and trainer requirements. Data created in Templates is used in Scheduling, Trainer and Resource Management and assessment and validation.

c. **CA.** CA includes functionality to administer courses and trainees, manage resources, trainers and accommodation and conduct trainee tracking and pipeline management. Data is exchanged between these functions, with DRS, scheduling, CME and JPA.

d. **PST.** PST supports the process of adding the correct number of courses to a schedule in order to meet the SOTT based on the SOTR for each Training Year (TY), while attempting to schedule courses to satisfying the training requirements within the resources available. Data from PST is exchanged with the CA module.

e. **Course assessment.** This supports InVal through the use of question banks, exams, statistics and scanning software. Results are displayed in CA modules.

f. **Course validation.** Provides functionality to Course Design Cells and TDTs to create and scan questionnaires in support of course evaluation and ExVal.

g. **Business Objects.** This is a management information tool that supports day to day reporting and management information reports.

h. **EMIS.** This is the corporate business intelligence capability in TAFMIS that extracts a sub-set of the data entered by users of the systems described above and is used to provide coherent management information.

i. **FOTIS.** This is a spreadsheet-based adjunct to TAFMIS that is used to produce the SOTR.

5 Defence Guidance for the TEL Ruleset[22]

5.1 Introduction

AIM

1. The TEL Ruleset describes the principles that are to be used for any development or implementation of TEL.

BACKGROUND

2. TEL is defined as technology used in training to improve the delivery of training in order to enhance learners' experience. Building on Chief of Defence People's direction[23], the 12 principles that make up the TEL Ruleset are based on the Government Digital Services (GDS) Technology Code of Practice (TCoP).

LINKED POLICY

3. Government Digital Services (GDS) Technology Code of Practice (TCoP) and DE&S Acquisition System Guidance (ASG) as part of the Acquisition Operating Framework. Also: JSP822; JSP440; JSP939.

5.2 The TEL Ruleset

4. To facilitate Cabinet Office approval, the 12 principles of the TEL Ruleset must be adhered to[24] as part of any business case when developing or procuring TEL for Defence[25]:

a. **Rule 1. Define user needs**[26]. TEL development[27] is to follow a flexible method which allows regular review between all stakeholders (such as managers, developers, sponsors, trainers, trainees etc) and draws on experience and innovation through the TEL Knowledge Hub. Project leads should understand the needs of the users and wider stakeholder requirements and examine a range of potential solutions to meet these needs. Furthermore, new TEL developments or procurements must clearly show a (documented) effort to meet wider Defence needs as well as TLB or role-specific requirements. Value for Money (VfM), capacity and capability (including any specific risk mitigation) must always be pre-eminent when delivering a new TEL solution and should be articulated with the perceived benefits of the new TEL solution in the business case.

b. **Rule 2. Make things accessible**[28]. New TEL should be accessible for users and by extension, training designers and managers. Consideration should be given

[22] JSP 604 requires ICT projects to be passed through Def Digital for approval. https://www.gov.uk/guidance/digital-and-technology-spend-controls-version-5
[23] As per the Foreword to JSP822 (See Volume 1).
[24] Each principle requires articulation on either how it will be met or the limitations that prevent it.
[25] The TEL Ruleset does not apply to Simulation. For Simulation refer to the DMaSC Ruleset in JSP939.
[26] https://www.gov.uk/guidance/define-user-needs
[27] Note that TEL development is specific to the development of TEL platforms / tools and is separate of the the development of learning content through the DSAT process that might then be hosted on / delivered through a TEL platform.
[28] https://www.gov.uk/guidance/make-things-accessible

to Specific Learning Differences, wider disabilities and Digital Literacy of those using and developing training by means of TEL. Additionally, attention should be made towards the potential training and upskilling of trainers and wider support staff on new TEL.

c. **Rule 3. Be open and use open source**[29]. If reuse of extant TEL and associated software is not possible, analysis of available license-free TEL must be evident when considering new TEL requirements. Licence free software such as Open Source (code which can be changed without restrictions) and Freeware, offer the opportunity for cost-effective TEL with no on-going licence fees (some Freeware is only available for personal use); however, due consideration must be given to the security of MOD data and systems.

d. **Rule 4. Make use of open standards**[30]. To inform Cabinet Office spend control process, Defence TEL solutions should use open standards to ensure they work and communicate across the Defence Learning Ecosystem with other Defence and external IT systems as required and can easily be upgraded and expanded to meet evolving and future requirements. This includes but is not limited to the standards defined by IEEE and the associated Learning Technology Standards Committee – see Table 1 below[31].

(P1484.1) Conceptual Model for Learning Technology Systems (CM4LTS)
(P1484.2) Interoperable Learner Records (ILR) Recommended Practices
(P1484.20) Competency Data Standards
(P1484.20.2) Recommended Practices for Defining Competencies
(P1484.20.3) Standard for Reusable Competency Definitions
(P1589) Augmented Reality Learning Experience Model
(P2247.1) Adaptive Instructional Systems (AIS)
(P2247.1) AIS Conceptual Modeling Subgroup
(P2247.2) AIS Interoperability Subgroup
(P2247.3) AIS Recommended Practices for AIS Evaluation Subgroup
(P2247.4) Ethical Considerations Subgroup
(P2384) Secure and Trusted Learning Systems
(P2881) Standard for Learning Metadata
(P2997) Enterprise Learner Record
(P7004) Child and Student Data Governance (CSDG)
(P7004.1) Virtual Classroom
(P7919) Standards for Mobile Learning Technology
(P9274) Experience API (xAPI)
(P9274.1.1) JavaScript Object Notation (JSON) Data Model Format and Representational Stat Transfer (RESTful) Web Service for Learner Experience Data Tracking and Access
(P9274.4.2) xAPI Cybersecurity
Other non-IEEE standards: Learning Tools Interoperability | IMS Global Learning Consortium

Table 1: Open Standards

[29] https://www.gov.uk/guidance/be-open-and-use-open-source
[30] https://www.gov.uk/guidance/make-use-of-open-standards
[31] JSP 939 Defence Modelling & Simulation Policy also provides links to open standards.

e. **Rule 5. Use Cloud first**[32]. If feasible, under JSP 440 and GDPR guidelines, public cloud should be considered in the first instance as per Government direction. Alternatively, if this is not feasible then sufficient justification to why the procured TEL should or could not use public cloud.

f. **Rule 6. Make things secure**[33]. Systems and data must be within prescribed Government Security Classification policy and wider Defence Security requirements[34]. Local unit ITSO and SCIDA points of contact should assist with this analysis for TEL security and associated activities including timelines.

g. **Rule 7. Make privacy integral**. Adherence to the General Data Protection Regulation should be an integral part of any current or new information system. Assistance through the application of Privacy Impact Assessments as part of the TEL procurement is recommended[35].

h. **Rule 8. Share and reuse technology**[36]. Existing TEL is to be used if it has been previously procured or designed. Many fully accredited TEL instances have been purchased for MoD use and include the DLE and VLE instances as well as enterprise licenses for authoring tools and 3D simulations such as VBS3. Defence is also required to utilise extant wider Government resources, such as Civil Service Learning products for generic learning requirements and ICS catalogue for commercial hardware, software and services which are common across government.

i. **Rule 9. Integrate and adapt technology**[37]. New TEL systems should be interoperable with existing technologies, infrastructure and organisation where possible. Good integration enables new technology to work with legacy systems, without limiting the ability to adapt to future demands or upgrade systems. Integration should allow the ability to create, share and adapt learning content and exchange data with other systems and effective planning should identify capability and process gaps. Exceptions to this can only be approved through the Defence Modelling and Simulation Coherence (DMaSC) Rules[38].

j. **Rule 10. Make better use of data**[39]. Consideration should be given towards the minimalisation of data collection and reuse of data to avoid duplication of datasets and optimise exploitation of information (i.e. within Training Management Information Systems and across such systems) within Government regulations.

k. **Rule 11. Define your purchasing strategy**[40]. The purchasing strategy must show consideration towards commercial and technology aspects and contractual limitations. Procurement of new TEL should be justified via the submission of a Business Case with approved means of In-Year funding and, importantly, future sustainment. TEL Project leads should engage with their respective Commercial representative at the earliest opportunity to exploit current contracts and opportunities before exploring bespoke procurement, but noting the following:

---

[32] https://www.gov.uk/guidance/use-cloud-first
[33] https://www.gov.uk/guidance/make-things-secure
[34] As per JSP 440.
[35] https://www.gov.uk/guidance/make-privacy-integral#how-to-embed-privacy-by-design
[36] https://www.gov.uk/guidance/share-and-reuse-technology
[37] https://www.gov.uk/guidance/integrate-and-adapt-technology
[38] Detailed in JSP 939.
[39] https://www.gov.uk/guidance/make-better-use-of-data
[40] https://www.gov.uk/guidance/define-your-purchasing-strategy

(1) Avoid customising off-the-shelf products and services in a way that inhibits their maintenance, upgrade or removal in future.

(2) Suppliers must not provide either: systems integration, service integration or service management services, at the same time as providing a component service within that system.

(3) Existing enabling agreements ensure that approved suppliers are used who satisfy Government or Defence requirements. These agreements are managed and reviewed to ensure that VfM and quality are maintained. If existing agreements do not meet the TEL requirement then the Acquisition System Guidance (ASG)[41] for new contracts is to be followed in conjunction with the TEL Ruleset, which includes the ability for projects to run their own commercial competition under the direction and guidance of an allocated Commercial Officer.

l. **Rule 12. Meet the Digital Service Standard for digital services**[42]. If the TEL project or programme includes the creation of a service, then the GDS Standard should be adhered to. This includes the adoption of Agile procurement methods[43] and the ownership of code, including intellectual property rights (IPR) should be understood and documented.

[41] Further guidance can be found in the Introduction to Commercial Matters for all Involved in Defence Acquisition (dated Aug 2018).
[42] https://www.gov.uk/service-manual/service-standard
[43] https://www.gov.uk/service-manual/agile-delivery