



Transformation Partners
in Health and Care
Digital Productivity



Digital Productivity Platform (DPP) Service Definition Document

Powering efficiency in the public sector



Contents

Section 1: Introduction to the Digital Productivity Platform	4
About us	4
Meet the Digital Productivity team.....	4
The Digital Productivity Platform (DPP) - an overview.....	4
Benefits of the DPP	5
A team you can trust.....	7
Our services.....	8
Recruitment automation starter service	8
Tailor-made workflows.....	9
Fully managed service.....	10
Next steps	10
Section 2: Professional services.....	12
Professional services explained	12
Six stage automation lifecycle - overview.....	13
Six stage automation lifecycle - development phases	14
One: Discovery	15
Two: Process definition	15
Three: Technical solution analysis	16
Four: Development and scenario testing	16
Five: Soft go-live.....	17
Six: Managed service (BAU)	17
Section 3: Onboarding	18
Key stakeholders	18
Onboarding the Digital Productivity Platform	19
RACI matrix.....	20
Section 4: Service model	21
Roles and responsibilities	21
Azure infrastructure	21
Cyber assurance.....	24
Virtual machine specifications	24
Robot types.....	25

Site to site IPSEC tunnel	26
Security standards for network rules.....	27
Technical controls.....	27
Section 5: Operational Support.....	30
Section 6: Connect with us	35
Appendix: Service catalogue	36
Clinical processes - primary care.....	36
Clinical processes - secondary and community care.....	37
Recruitment automation service.....	40
Non-clinical processes.....	42

Section 1: Introduction to the Digital Productivity Platform

About us

Who we are: Transformation Partners in Health and Care (TPHC) is an NHS consultancy that specialises in a range of strategy, business change and transformation services for health and social care, including data analysis, population health management, digital enablement and pathway redesign. Hosted by the Royal Free London NHS Foundation Trust (RFL), we work side-by-side with partners across the system to deliver tangible, lasting results for the populations they serve.

The internal advantage: Choosing TPHC means reinvesting resources and expertise back into the NHS. As a publicly owned, values-driven alternative to private sector consultancy, we provide a cost-effective service rooted in a deep, lived understanding of the system's pressures and priorities.

Our mission: Through our talented multi-disciplinary teams, we harness a unique blend of expertise to deliver positive change and maintain an outstanding track record of success - from local neighbourhoods to national-level programmes.

Meet the Digital Productivity team

Our origin: Our journey began in 2020 as the Automation Centre of Excellence, funded by NHSX and hosted within the Royal Free London. After onboarding a team of highly skilled developers and specialists and investing in technology, we have successfully delivered over 100 automations for more than 50 NHS organisations.

Our growth: Since joining TPHC in 2023, we have evolved into a specialist hub for intelligent automation. By listening to our customer's most pressing challenges and learning lessons from our work across the NHS, we designed and deployed the **Digital Productivity Platform (DPP)**, built to address the specific challenges of the public sector.

Expertise and recognition: We are a team of substantive NHS professionals with a proven track record of delivering incredible results. Our work has been recognised with multiple awards for its dedication to improving NHS efficiency and patient outcomes.

The Digital Productivity Platform (DPP) – an overview

What it is: The DPP is a first-of-its-kind, NHS-led, cloud-based solution. It enables organisations to automate manual, repetitive tasks flexibly and affordably through a scalable, pay-as-you-go model.

The vision – making time matter: We provide cutting-edge, outcome-based solutions that help our public sector colleagues save time and work more efficiently.

Through this approach, we seek to make digital productivity as a service accessible to everyone in the public sector, irrespective of an organisation's size, financial status or technical proficiency.

Benefits of the DPP

 Leading technology Orchestration The DPP boasts cutting edge AI orchestration – 24/7 platform health and process performance monitored and managed automatically.	 SLA driven Value for money SLA driven productivity provides total control – Bot capacity instantly flexes to match demand, which means when it's not in use there are no charges being incurred, offering true economy of scale.	 Fully managed Light touch The DPP takes away need for internal resources to monitor, maintain, break fix and change the environment and its processes. All costs wrapped into per minute costs	 Service desk Single point of access Local level support for all break fix and change requests. Our dedicated team offers support and service matched to your needs. Often issues are handled before client is even aware.	 PMO support Customer success The DPP account team ensures all stages of service delivery, design, development, deployment, monitoring, KPIs and SLAs are effectively managed and reported on as required.	 Assurance Your data protected Connected via an IPSEC VPN, the DPP is an ISO 27001 compliant solution. Our team of substantive NHS staff assists with all IG and DPO requirements, providing cyber and data assurance against our CE+	 Multivendor Flexible Masters of their craft, the DP team uses a range of market leading tools. With this broad technology stack at our disposal the DPP delivers outcomes using the most appropriate solution for your business needs.	 NHS awareness 50 years of collective experience Over 50 NHS organisations have trusted the DP team to provide consultancy, design, development, and operational support across all sectors and service lines.
--	---	---	---	--	---	---	--

Acronyms: AI = artificial intelligence; SLA = Service Level Agreement; PMO = Project Management Office; IPSEC VPN = Internet Protocol Security virtual private network; IG = information governance; DPO = Data Protection Officer; CE+ = Cyber Essentials Plus; DP team = Digital Productivity team

Core benefits:

- **Economical:** Our consumption-based model means you only pay for what you use. There are no high upfront costs, wasted capacity or long-term commitments, making this an affordable and sustainable solution which provides true economies of scale.
- **Fully managed:** We remove the technical burden. Our team provides 24/7 AI-powered orchestration and monitoring to ensure consistent, reliable performance.
- **Enhanced staff wellbeing:** By replacing manual repetitive tasks with digital workflows, we reduce staff burnout and the potential for human error, allowing your workforce to focus on high-value patient care.
- **Clinical and non-clinical processes:** Our intelligent automation scales across HR, finance, primary and secondary care, mental health, and beyond

A team you can trust

Proven impact: Our team of digital pioneers has delivered tailored automations that have delivered significant, measurable capacity back to the system. For example, in 2024/25:

- Shared services recruitment: We delivered 36 automations, saving over 33,000 hours (28 WTE) and processed 283,000 items.
- Clinical pathways: A project for chronic kidney disease referrals released 142 working days of clinical time and reduced the risk of human error.



Reliable support: We provide a single point of support via our dedicated team. Our proactive monitoring approach means we often identify and resolve issues before they can impact your service, ensuring a seamless experience for your teams.

Our services

We have three core service offerings:

1. Recruitment automation starter service
2. Tailor-made workflows
3. Fully managed service

Each service is discussed in more detail below.

Recruitment automation starter service

How it works

- **Ready-built automations:** Choose a process from our starter service catalogue of standard NHS workflows, for example, workforce employee checks.
- **Pay as you consume:** Only pay for what you use. Our flexible pricing model works on a per-minute basis, allowing the scaling of usage according to business demand, without worrying about under used and expensive capacity
- **Seamless integration:** Our automations integrate with existing internet-facing systems and workflows, ensuring a smooth, hassle-free experience.
- **Real-time analytics:** Monitor and track automation performance with detailed analytics and insights through targeted reporting to quickly and efficiently report on key performance and outputs.

Key benefits

- **Cost-effective:** Avoid hefty investments in custom automation development or software licenses. Through SLA's you control the costs and only pay for the actual process minutes, not the capacity.
- **Scalable:** Whether you are processing hundreds, thousands or even millions of transactions, our automations can instantly scale to meet business needs, supporting growth without the need for additional resources.
- **Rapid deployment:** With no lengthy implementation process, we can deploy our automations quickly, allowing you to start seeing benefits almost immediately.

Tailor-made workflows

How it works

- **Custom automation development:** We collaborate with the customer to understand specific needs and create bespoke automations to precisely replicate the customer workflows.
- **Secure point-to-point VPN:** To ensure the highest level of data security and privacy, we establish a dedicated point-to-point VPN between our infrastructure and the customers. This secure connection allows us to access customer systems safely, ensuring the integrity and confidentiality of data during the automation process.
- **End-to-end process flow design:** From initial consultation to deployment, our team of automation experts designs and implements custom process flows that are fully aligned to business needs. To facilitate this, we use our [six stage automation lifecycle methodology](#) to ensure data is handled in a responsible, professional, and safe way.

Key benefits

- **Highly customised solutions:** Our service is fully bespoke, allowing us to create automation solutions that are perfectly aligned to the specific business needs and strategic ambitions of your organisation.
- **Enhanced security:** With a dedicated point-to-point VPN, we provide a secure environment for automation development and execution, safeguarding sensitive data at every step.
- **Deep integration:** Our bespoke automations are built to integrate deeply with your existing systems, ensuring seamless operation without disrupting current workflows.
- **Scalable and adaptable:** As the business grows and evolves, our bespoke automations can be scaled and adapted to meet changing demands, ensuring long-term value and efficiency.

Fully managed service

How it works

- **Migration of existing processes:** We undertake a review of your existing automation estate and once approved provide financial modelling against our pay as you go model.
- **Peace of mind:** The DPP offers customers a fully managed service freeing you of the operational burden of more traditional automation platforms. Utilising a fully orchestrated service driven model digital workers flex to meet your demand ensuring resource is always available. With robust customer service and 24/7 AI monitored orchestration your DPP managed service provides ultimate peace of mind.
- **Pay for what you use:** The DPP model allows up and down scaling of resources, you therefore never pay for underused virtual worker capacity, meaning return on investment is not compromised due to an idle digital workforce.

Key benefits

- **Service driven digital productivity:** AI powered orchestration ensures 24/7 monitoring and response to your business need. Virtual machines (VM) can be spun up/down, terminations retried, and workers logged back in. Over runs and schedule bottlenecks become a thing of the past.
- **NHSE secure:** DPP uses the newly released Secure Robot Authenticator with CIS2 to provide seamless and secure access to NHS spine applications
- **Transparent contracting:** With contract durations to suit any organisation, DPP offers the ultimate solution for business wishing to scale existing ecosystems of digital productivity tools or simply provide short term proof of concept.
- **Scalable and adaptable:** As the business grows and evolves your digital workforce can be scaled and adapted to meet ever-changing demands, ensuring long-term value and efficiency through true economy of scale.

Next steps

This Service Definition Document will guide you through our standard implementation journey, clearly setting out the critical roles and responsibilities for us as the solution partner and you as our valued customer to facilitate a smooth onboarding and operational deployment.

The document is split into helpful sections that provide deeper insights into all key aspects of the platform.

Ready to transform? If you are ready to learn more about how the Digital Productivity Platform can add value to your organisation, [visit our website](#) for case studies, or get in touch to discuss your specific requirements.

Please contact the Digital Productivity Team at rf-tr.dpp@nhs.net.

All that remains is to say thank you, and let's begin.

Section 2: Professional services

Professional services explained

The Digital Productivity team have a long history of delivering award-winning, tailor-made process automations. Our professional automation services are available in two ways:

Customer environment

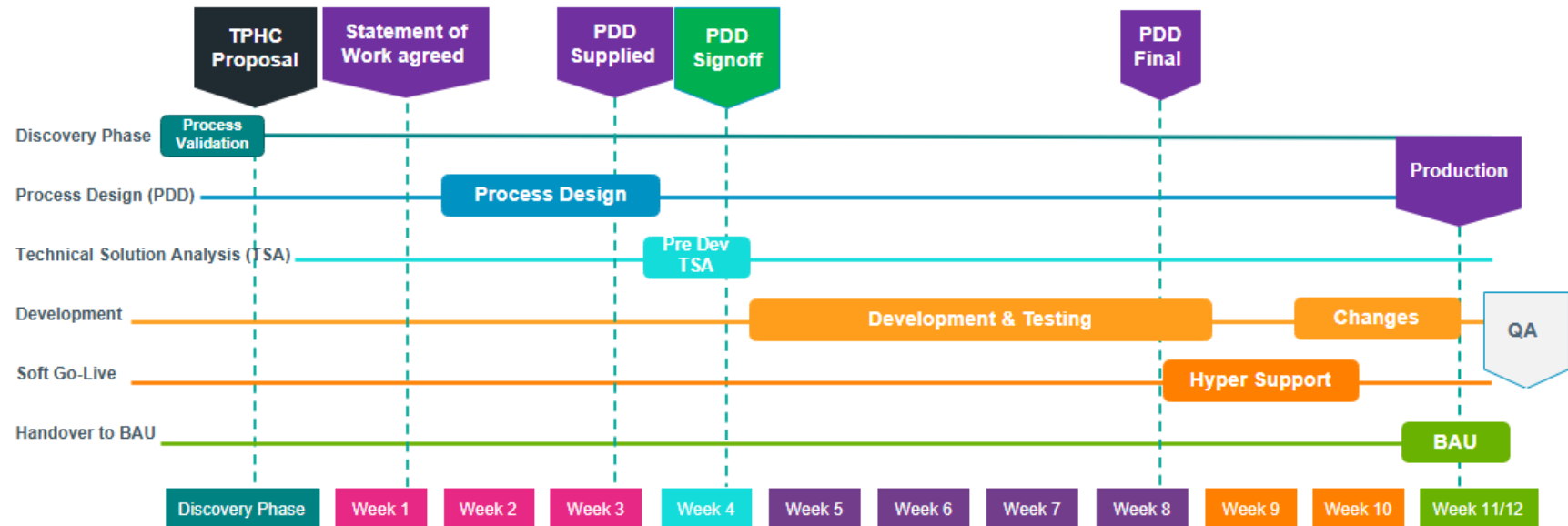
- The Digital Productivity team have designed, developed, deployed and supported over 110 automations to customer environments across clinical and non-clinical service lines for all sectors of the NHS. Working to world-class best practice and quality assured standards we work closely with our customers to deliver processes that are fully compliant to information governance (IG) and clinical safety requirements.
- We are experienced in achieving NHS Digital DCB0160 compliance with clinical automations and we work to ensure organisational data protection impact assessments (DPIA) and service level security policy (SLSP) are achieved. Where customers do not have in-house expert resource the Digital Productivity team provide operational support services to maintain the automation environment and the processes within it.

The Digital Productivity Platform

- For customers who do not have an in-house automation environment the DPP is the perfect service. Once onboarded as a fully managed service, the DPP is relatively light touch for digital and network teams, making it the perfect choice for customers needing to access automation without the operational burden and resource demands of an in-house platform.
- Automations designed and developed for consumption-based delivery follow the same design and development principles of the six-stage automation lifecycle, but then rollout to DPP for consumption-based delivery. The following pages set out the Digital Productivity team's delivery methodology.

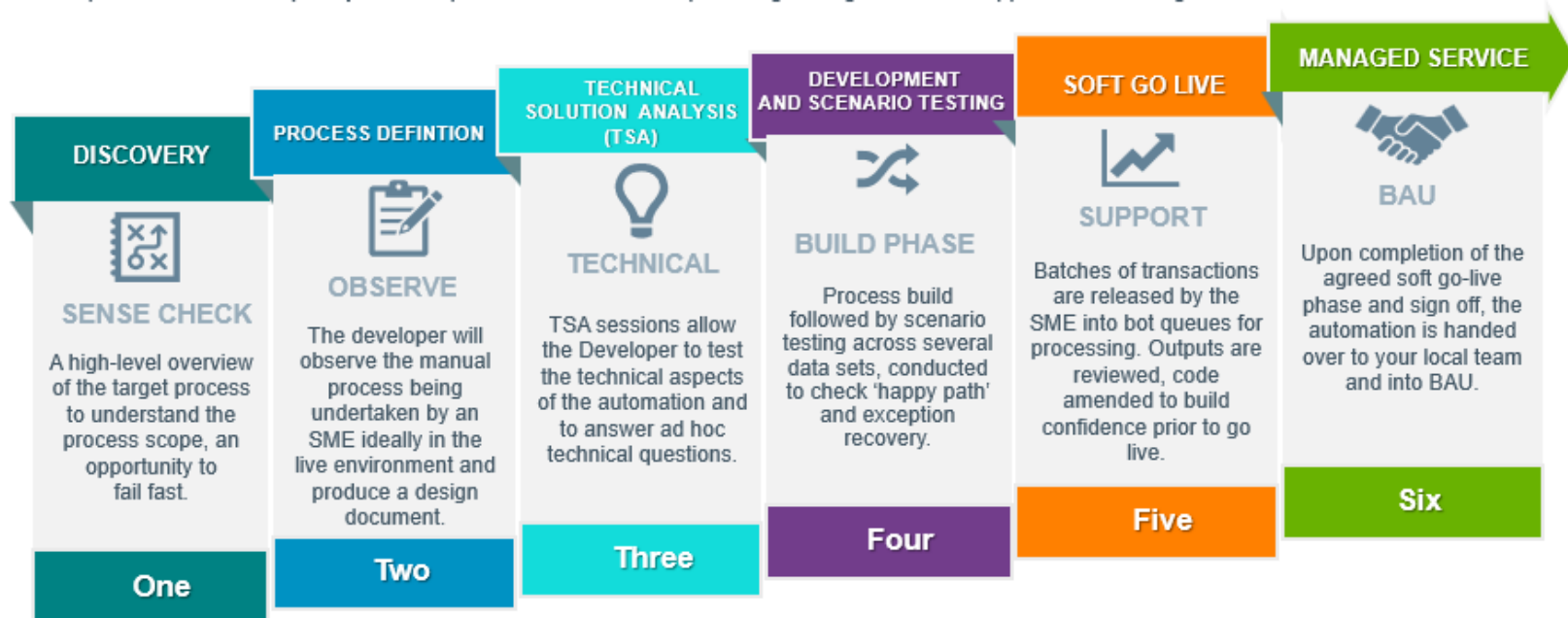
Six stage automation lifecycle – overview

Customers requiring tailor-made solutions will be taken through our six-stage automation cycle. The following diagram provides a typical journey for a process of mid-complexity. Clinical processes will often require longer for governance support and more rigour around data validation.



Acronyms: TPHC = Transformation Partners in Health and Care; PDD = Process Design Document; Pre Dev TSA = Pre-development Technical solution analysis; QA = Quality assurance; BAU = Business as usual

Six stage automation lifecycle – development phases



Acronyms: SME = subject matter expert; BAU = business as usual

One: Discovery

Customer responsibility:

- Subject matter expert (SME) and process owner resource availability. For this session to be successful the developer needs to see the end-to-end as-is state of the process, these sessions can identify challenges and immediate barriers to automation.
- Metrics – to fully understand the capacity demands of the process, and to assist in your own benefit reporting/profiling, we recommend you collate the base metrics of the process, these being the volume, frequency and an accurate time in minutes to complete the manual process.
- Understand internal requirements/governance for appropriate testing, which we refer to as the ‘testing threshold’. It is vital that internal teams, such as IG and clinical safety are engaged early in the process to help define the user acceptance criteria.

Digital Productivity team responsibility:

- Following the walkthrough session, the account team will produce a proposal in writing in the form of a statement of work. This document will provide a fixed price cost and estimated delivery time, which is subject to confirmation of existing automation platform availability and our standard access requirements in order to complete a system health check.

Two: Process definition

Customer responsibility:

- SME and process owner resource availability. This session requires the developer to be provided a granular level walk through, click by click of the predefined ‘happy path’ of the process. This requires your internal agreement to both the scope and acceptance of the process, scope creep at this stage will prolong the entire definition process.
- To provide access to test or live data to provide a real-world view of the process including known and/or possible exceptions. Please note that the sessions are recorded to allow time to review and capture every aspect of the process.
- Ensure that details of all systems and applications used by the process are provided to the developer for inclusion within the PDD. This also being a prerequisite for the process moving into development.
- To provide timely feedback and responses to requests for further information, PDD review meetings and document iterations and finally PDD sign off.

Digital Productivity team responsibility:

- Ensure sensitive data is protected e.g. recordings and screen shots in line with the data processing agreement.
- To represent an accurate understanding of the business process within the PDD.

- Provide the first iteration of the PDD. PDDs rarely receive sign off from the first draft, to maintain momentum it is vital the SME resource is aware the PDD is an iterative process throughout the entire lifecycle of the automation build.
- Complex processes such as those using multiple clinical systems may require an extended PDD creation time.

Three: Technical solution analysis

Customer responsibility:

- SME and process owner resource availability for TSA session.
- To provide timely feedback and responses to any developer requests for further information.

Digital Productivity team responsibility:

- At this stage, the developer will prepare further technical questions and ensure all pre-development prerequisites are signed off, this includes such things as specific application access e.g. Outlook, Excel etc. Along with all the necessary access credentials such as virtual smart card or PAS system patient administration system details.
- Outcomes from the TSA will be added into the PDD by the developer and signed off by the customer. This may require further iterations as the development progresses through its lifecycle.

Four: Development and scenario testing

Customer responsibility:

- It is not uncommon during the development cycle for issues to arise, which can be for a variety of reasons. To ensure the build continues at pace, please ensure SME resource continues to be available and responsive to any developer requests, these may be via email or virtual meeting discussions.
- Stakeholder engagement – our extensive experience across the public sector has taught us that engagement and buy-in from all stakeholders is vital for programme success, at every level of the organisation.
- To provide timely feedback and sign off to PDD iterations.

Digital Productivity team responsibility:

- To provide regular updates on build process, this includes highlighting issues and challenges.
- To ensure the PDD continues to be iterated through the entire build process and captured within the PDD document control.

- Change request to 'inflight' developments will require an update to the PDD along with additional SME sign off. Changes at this stage may also be subject a contract variation within the statement of work.

Five: Soft go-live

Customer responsibility:

- It is not uncommon during the soft go-live phase for issues to arise, these can be for a variety of reasons such as a new application pop-up or a data quality issue. To ensure the soft go-live is successful we will require timely responses to questions from the developer.
- On a pre-defined basis, the SME is required to validate the bot outputs in the host applications and match this against the output report from the bots.
- To ensure customer processes are in place to handle valid business exceptions requiring human input.
- To have a clearly defined business continuity plan in place in the unlikely event of a service interruption.

Digital Productivity team responsibility:

- To provide regular updates on bot performance and issue exception reports at the end of each defined period.
- To liaise with the customer at the start of each transaction run to avoid any duplication between human and robot.

Six: Managed service (BAU)

Customer responsibility:

- It is now time to migrate your new process into production, this may be in your own automation environment, or to our consumption-based Digital Productivity Platform. The development team will have completed debug testing and process stabilisation in readiness for the production rollout.
- A final sign off meeting will be conducted with the developer to complete the automation lifecycle and receive final sign off for delivery.
- To provide timely feedback and sign off to go-live approval.

Digital Productivity team responsibility:

- Handover document – this document, which is a final iteration of the PDD with further technical notes acquired along the development cycle are handed over from the team.
- DPP delivery – to provide regular output reporting to agreed schedule and SLAs
- Maintain process as agreed maintenance including break fix, monitoring, and change request.

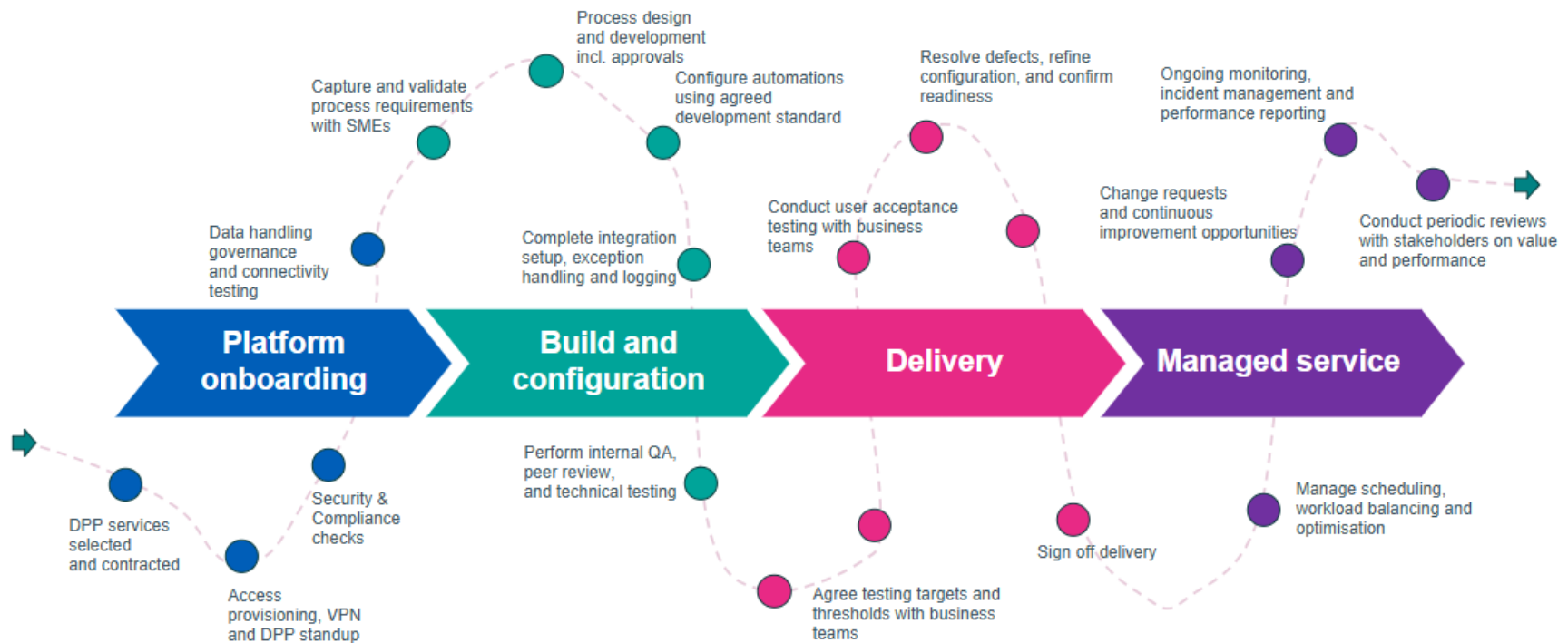
Section 3: Onboarding

Key stakeholders

Successful onboarding relies on early intervention with all internal stakeholders; the following list is a guide to assist you with these engagement activities.

Role	Function	Point of Engagement
SME	SMEs play a vital role in onboarding and process deployment, they are involved in all aspects of the automation lifecycle, go-live and post go-live activities.	Initial discovery onwards
Regulatory Affairs (RA)	Processes that will require access to authenticated systems such as Electronic Staff Record (ESR) or other NHS spine applications will be required to have RA approval.	Process selection and validation and design stage
Cyber Security Lead	Your security team will be interested in the platform architecture, how it is built and what controls are applied, including how the platform operates normally and through a security incident. Your security team may need to be involved with discussion about data handling during the onboarding and individual project phase.	Procurement stage
IG Lead	Your IG team will need to work with you to complete a data protection impact assessment (DPIA) and data sharing agreement (DSA). There may be other local compliance to achieve.	Procurement stage
Clinical Safety Officer (CSO) - clinical processes only	Ensuring all aspects of clinical safety are considered and compliance with DCB0160 standards are achieved for any process automation that handles patient data.	Process selection and design, CSO involvement at this stage is critical.
Digital / IT / Networking	Provide critical support to onboarding as key enablers to VPN connectivity and testing procedures, they will also lead on system/application and data access requests.	Initial discovery onwards

Onboarding the Digital Productivity Platform



Acronyms: DPP = Digital Productivity Platform; VPN = virtual private network; SME = subject matter expert; QA = quality assurance

RACI matrix

Successful onboarding relies on early intervention with all internal stakeholders, the following list is a guide to assist you with these engagement activities.

Activity	Exec Sponsor	Digital / IT	Cyber Security	IG / DPO	Clinical Safety	Networks / Infrastructure	Ops Lead	DPP Team
Environment setup	I	A/R	C	I	I	C	I	R
Platform access and permissions	I	A/R	C	C	I	C	I	R
Cybersecurity	I	C	A/R	C	I	C	I	C
IG, compliance etc.	I	C	C	A/R	C	I	I	C
Clinical safety	I	C	C	C	A/R	C	I	C
Governance	A	R	C	C	C	C	C	I

Section 4: Service model

Roles and responsibilities

The DPP uses industry leading technology and AI to continually monitor the DPP environment and its live processes while dynamically orchestrating work queues, and optimising outputs continually, day and night seven days per week.

Digital Workers are automatically reset if they freeze, go offline or are hit by a performance issue because of overruns. During office hours the dedicated service desk team ensures support requests are prioritised against a robust service level agreement giving further peace of mind. It is important to note the roles and responsibilities surrounding an affective managed service.

DPP team responsibilities:

- Management of the DPP Azure environment
- Incident and support management
- Capacity and performance management
- Cloud access management and security control
- Patching
- Process build, change, and configuration management
- Performance monitoring and reporting

Customer responsibilities:

- Notifying of business application updates and downtime
- Provision of test data and testing outcomes
- Benefit reporting and KPI metrics

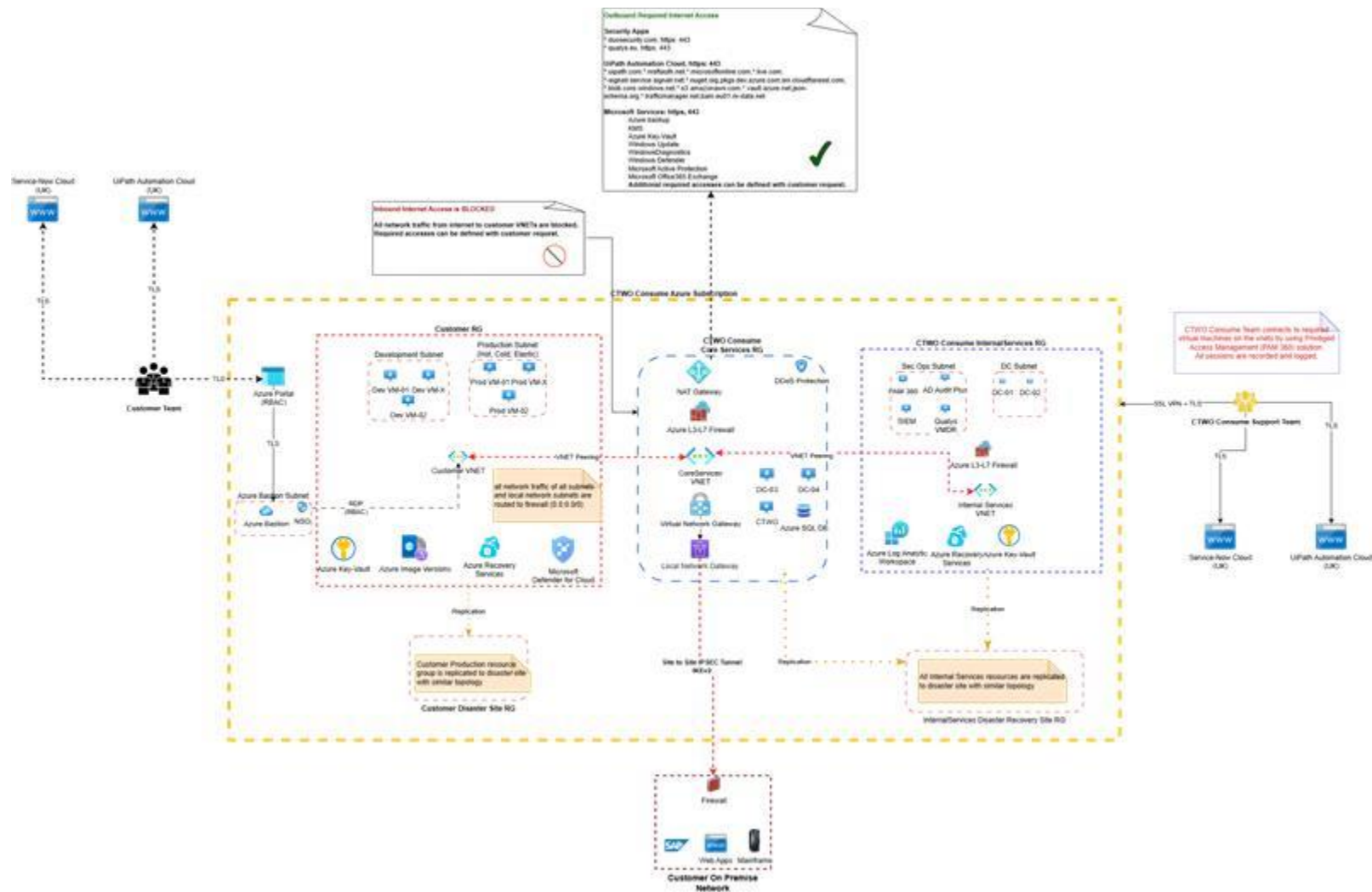
Azure infrastructure

The DPP core product set is hosted on ISO (27001, 9001, 20000), SOC2 and UK General Data Protection Regulation (GDPR) certified compliant infrastructure. For each customer, distinct resource groups are established within the DPP's Azure subscription and geographically compliant within the UK region.

All automation environments which include Development, user acceptance testing, Regression, and Production are isolated within the customer Azure Virtual Network (VNet) and dedicated to individual customers, enhancing network security and isolation.

The illustration below shows a secure cloud infrastructure setup for the DPP's core services. Key elements include:

- Core digital productivity services are segregated into dedicated resource groups within Azure.
- Inbound and outbound network traffic from the internet to customer dedicated VNets are blocked by default and only amended in line with target process needs ensuring minimal exposure to external threats.
- Where target processes require access to customer applications a secure IPSEC Site to Site VPN tunnel will be established protecting the communication between the Azure Data Centre and the customer's on-premise infrastructure ensuring all data exchanges occur over encrypted channels.
- Disaster recovery sites detailed for business continuity and disaster planning, ensuring the platform remains operational even in the case of critical failures, minimising downtime and data loss.
- Access is restricted to authorised individuals only.
- Overall, this infrastructure supports secure and reliable automation services by enforcing strict network access controls, ensuring encrypted connections and implementing robust disaster recovery strategies.



Cyber assurance

The DPP is governed and protected through the following standards:



Virtual machine specifications

An Automation Runtime VM is a dedicated end-user desktop environment designed to emulate human workflows for automated tasks. It provides the necessary virtual infrastructure, including CPU, memory, and storage, to run bots or scripts that replicate manual processes, such as data entry or application interaction.

This VM mimics a typical user desktop to ensure that automation behaves as a human would in real-world scenarios, allowing for seamless execution of tasks without human intervention.

1. Base VM Image Template

- The DPP offers VM image templates based on a pre-built standard configuration to include browsers, Office 365 applications and core RPA products.
- When onboarding a new customer, a new machine can be generated from these base VM image templates. After installing necessary customer applications and settings, access tests are performed.
- A customer specific image is then created and deployed on the DPP.

2. Customer's image template

- Azure Services Image Sharing: If a customer utilises Azure services, they can share a pre-created image for replication. Alternatively, the customer can provide us with the virtual hard disk (VHDx) format of their image. This image file is then uploaded to our designated Azure Blob Storage.

DPP typical VM specification:

- Windows Server 2022 Datacentre Azure Standard Operating System
- B2Ms (Azure B-Series Burstable VMs)
- 2vCPUs (Virtual CPUs)
- 8GB RAM (random-access memory)
- Office Products
- SAP
- Browsers
- Anti-virus

Robot types

All production robot VMs, regardless of their image source, are equipped with a reboot-to-restore mechanism to prevent any unintended misconfigurations. This ensures optimal security by removing customer files and eliminating potential malware infections upon each reboot.

Based on the customer requirements, the DPP provides the following robot types:

1. **Hot Robots (Ready VMs):** Hot Robots are provisioned, running, configured and available for jobs when needed.
2. **Cold Robots (Deallocated VMs):** Cold Robots are provisioned and configured but in a deallocated state.
3. **Virtual (Elastic) Robots: *Allocated on-demand VMs:*** Using a pre-defined VM image, a template is made to create machines on demand whenever a robot needs to run a job. Customers can apply limits on how many machines can be created and when, then we will do the rest.

Robot Type	Hot	Cold	Virtual
T (min) to ready	0	~2-3	~10
Robot status	VM Provisioned, Robot Installed, Robot Registered, VM Started, OS Ready (services started)	VM Provisioned, Robot Installed, Robot Registered, Start VM, OS Ready (+ Robot Service)	VM Provisioning via template, Robot Installation, Orchestrator Connection, Start VM, Load OS (+ Robot Services)
Machine scaling	Limited to the number of machines provided	Limited to the number of machines provided	As many machines as needed to optimally handle the workload with customers pre-shared parameters
VM setup	Set up multiple individual VMs	Set up multiple individual VMs	Set up a single VM Image
Start and stop VMs	Always run	Automated	Automated
VM customisation	Customise the VMs you use (domain-joined, machine size, machine name, network options and more)	Customise the VMs you use (domain-joined, machine size, machine name, network options and more)	VM Image must be configured as recommended
Machine provisioning	Manual	Manual	Automated

Site to site IPSEC tunnel

When customer-specific workflows require access to applications or resources not available over the internet, a site-to-site IPsec VPN tunnel can be established. This secure connection enables seamless communication between the platform and the customer's on-premises network. In line with best practices, a compatible VPN device is required to configure the cross-premises VPN connection, ensuring robust, encrypted data transmission and maintaining security standards between both environments.

Compatibility:

The DPP is compatible with Microsoft supported devices only.

Please see below for list of compatible devices and Azure Security baseline information:

- [About VPN devices for connections - Azure VPN Gateway | Microsoft Learn](#)
- [Azure security baseline for VPN Gateway | Microsoft Learn](#)

Process:

- Customer completes a request form and returns to support team
- Request form validated and confirmed
- PSK Share
- DPP VPN configuration
- Customer VPN configuration
- Access test and validation

IKE Phase One	IKE Phase Two
• Encryption: AES-256 • Integrity (HMAC): SHA-256 • DH Group: Group 14	• Encryption: AES-256 • Integrity (PRF): SHA-256 • PFS Group: ECP256 • About VPN devices for connections - Azure VPN Gateway Microsoft Learn

Security standards for network rules

The DPP operates a pinhole security model. Inbound and outbound traffic to the platform is allowed only via specified ports or protocols via Azure Firewall. 'Any' designation for destination, source, port or protocols are not allowed on the DPP.

The process specific network rules must be defined as example below in line with Azure Firewall best practice:

Application name	Source	Destination type	Destination	Protocol	Port	Action	Description
Example website	Digital Productivity Platform	FQDN	www.example.com	TCP	443	Allow	Allows access over HTTPS to the example site
Example website 2	Digital Productivity Platform	IP Address Range	203.0.113.0/24	TCP	80	Allow	Allows access over HTTP to the example site 2

Technical controls

Encryption at rest and transit	- The DPP embraces a robust encryption strategy for its Azure resources. - The core components of the platform, including Virtual Machines, databases and other resources are stored in an encrypted manner to safeguard sensitive information. - Additionally, encryption in transit via transport layer security (TLS) between Azure services and via VPN (where applicable) ensures data cannot be intercepted or tampered with during transmission.
IP Filtering for application-service access	- IP addresses/ranges are only whitelisted if from a trusted source and required for business process needs. - Only traffic from these IPs will be permitted reducing the risk of unauthorised access to the DPP.
Cryptography	- The DPP ensures the proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information. - Symmetric key encryption methods are used on both Microsoft SQL Databases and Queue Item Data that resides in the orchestrator (operational support product). - All robot and orchestrator communications are handled with TLS.
Malware protection	- All DPP virtual resources are protected against malware. - Exploits and malicious code via a centrally managed Endpoint Detection and Response (EDR) solution that is kept regularly updated, combined with appropriate user awareness and training.

Security patching and updates	• Critical security and OS updates are applied within 30 days of manufacturers release. • The use of the Qualys Vulnerability Management Detection and Response (VMDR) ensures vulnerability monitoring, vulnerability risk assessment and prompt patching. • Notifications of potentially relevant technical vulnerabilities are addressed within 12 hours, with high-risk system remediation prioritised.
Privileged account management and access control	• The Platform Support team and IT Security team are responsible for managing privileged accounts that are granted elevated permissions within the DPP. • These accounts undergo strict authorisation processes and are granted access based on the principle of least privilege. • This approach ensures that only authorised personnel can perform critical actions and tasks.
Restricted administrative access	• To mitigate lateral-movement, privilege escalation attacks such as pass-the-hash etc., a strategic approach is implemented within the DPP. • Domain/Enterprise administrator accounts are restricted from directly logging into servers and workstations. Instead, a robust practice is adopted where all administrative operations are carried out using local administrator accounts. • This approach serves as an additional layer of defence against potential attacks by minimising the exposure of highly privileged domain admin credentials. • By limiting domain admin access to servers, the risk of compromising these credentials is significantly reduced. Administrative tasks are channelled through local administrator accounts, thereby enhancing security and maintaining a controlled environment.
Regular password rotation for local admin accounts	• We facilitate the regular (daily) rotation of unique, complex passwords for each local admin accounts across all servers, workstations within the DPP via Microsoft Local Administration Password Solution (LAPS). • This proactive approach ensures that local account passwords are frequently changed.
Just-in-time admin access through service-now integration	• To maintain strict control over administrative access, the Platform Support team and IT Security team leverage the integration of PAM360 with Service-Now. • When administrators require access, they must set the approved ticket number on Service-Now. This request is meticulously verified, and access is granted only upon formal approval. • This just-in-time admin access ensures that administrative connections are closely monitored and controlled.
Automated password reset after each admin	• Upon the conclusion of just-in-time admin access, PAM360 automatically triggers a password reset for the accessed account. • This automated process enhances security by ensuring that each session is ephemeral, preventing the reuse of previously granted

access	access credentials.
Identity role-based access in automation cloud	• The DPP embraces a role-based access control framework to ensure precise and secure user permissions within the platform. • By implementing role-based access, customers can be assured that users are granted access only to the functionalities and resources essential for their roles.
Multi-Factor Authentication (MFA) for enhanced security	• We enforce all our staff by implementing Multi-Factor Authentication (MFA) across all access to platform when logging into applications, SSL VPN, RDP or Console sessions via both DUO MFA and Microsoft MFA.
Audit log monitoring	• We try to minimise the attack surface or mis-configuration issues of our services and to reduce the probability of a data breach ever occurring. • Our support team is always on hand to rapidly identify the issue from correlated audit logs privileged right escalations events and engage the necessary team resources to contain the impact of the incident. Standard support is available Monday through Friday 9:00am-5:00pm and excludes Bank Holidays.
Credentials management	• All robot account admin secrets we use to manage and maintain the service and robot runtime resource credentials are stored and transmitted securely through the Azure Key-Vault. • All secrets are rotated on a regular period and can be rotated on-demand if there is a security event. • All customer application credentials are stored securely on Orchestrator credential store.

Section 5: Operational Support

The Digital Productivity team is committed to supporting our customers in the event of issues and requests. As such the provision of Digital Productivity products are supported through a dedicated service and support process.

The following categories, and assignment group details help define how your requests are mapped and subsequently allocated to the most appropriate departments to be resolved as efficiently as possible.

Service Period	Tier	Assignment Group
Mon – Fri 09:00 – 17:00*	T1	DPP Project Management Office (PMO)
Mon – Fri 09:00 – 17:00*	T2	DPP Technical Team
Mon – Fri 09:00 – 17:00*	T3	DPP Senior Team
Mon – Fri 09:00 – 17:00*	T4	Solution Provider Escalation

* Excludes UK Public Holidays

Service categories:

- **Incident support:** Management of incidents and issue resolutions.
- **Change management:** Request for changes to hosted processes in Managed Service environments.
- **Reporting requests:** In the event ad-hoc reporting is required outside of your agreed monthly reporting schedule.
- **New process requests:** New developments into Managed Service and Hybrid environments.
- **Process start/stop:** For processes delivered in any of the DPP products

Email ticket management:

Service time	Initial Response	Group	Solution
Monday – Friday, 09:00 – 17:00	60 minutes	T1	Convert to incident
Monday – Friday, 09:00 – 17:00	60 minutes	T1	Convert to service request

Service requests:

Request category	Request handling		
	Response	Solution or referral	Initial response level
Process change request	1 working day	Referral to L2	T1
New report	1 working day	4 hours referral to L2	T1
Report	2 hours	4 Hours	T1
Scheduling change	2 hours	1 working day	T2
Onboarding new process	1 working day	Best efforts	T1
Start process	1 hour	2 hours	T2
Stop process	1 hour	2 hours	T2
General enquiry	1 working day	Best efforts	T1
Application downtime notifications	1 hour	4 hours	T2

Incident requests – process overview:

- Email ticket received, reviewed by Tier 1 PMO and a response returned within 60 minutes with next steps.
- On review PMO referral decision made using triage method to refer Tier 2 or Tier 3 – all DPP queries default to Tier 3 and incident details passed to the Senior Development Team.
- After review, early investigation and intervention, a decision will be made on next steps to resolve or escalate to Tier 4 SAAS partner services.
- The customer will be updated with actions to date and next steps.
- Tier 4 escalated within 90 minute SLA window – solution response then dependent on partner service response. Following this, the resolution / solution / escalation outcome is updated to the customer and the incident is closed.

Incident tiers:

- Tier 1 - DPP PMO (first line)
- Tier 2 - DPP Technical Team (Second Line)
- Tier 3 - DPP Senior Team (Third Line)
- Tier 4 - Solution Provider Escalation (Architects)

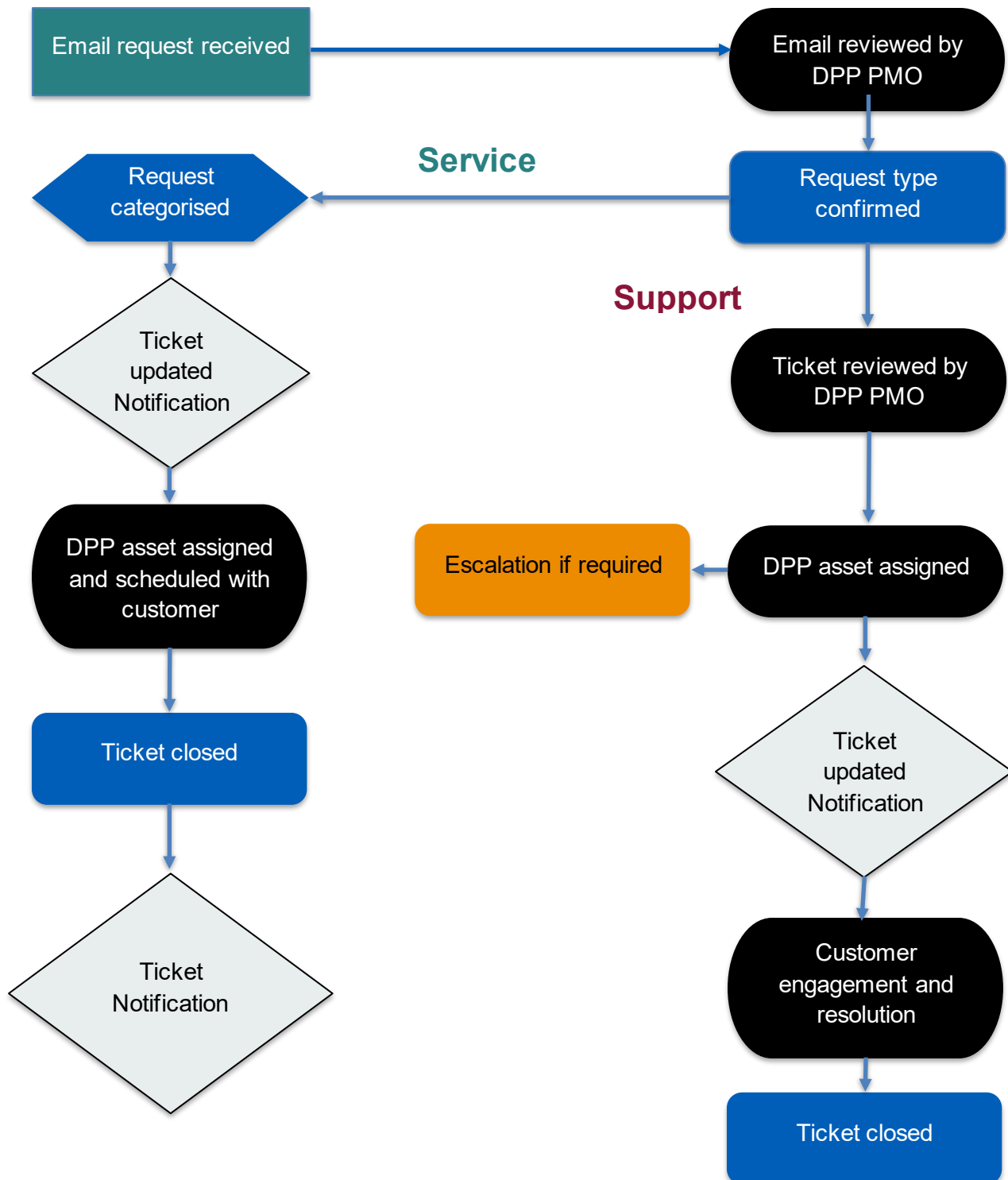
	Incident Handling			
	Service Level Agreement			
	Response + Solution			
	120 Minutes + X Hours			
	Tier 1 OLA			Group OLA
Time	Response	Group	Solution or Escalation	Response, Solution, Escalation
M to F (9-5)	30 mins	T1	90 mins	X Hours

Escalations:

In the unlikely event that an incident or request requires escalation the following contacts will be available Monday through Friday 9:00am – 5:00pm.

Role	Contact	Email
General Enquiries	PMO Office	rf-tr.tphc-digitalproductivitypmo@nhs.net
Support & Service Tickets	Service Desk	DPP.support@nhs.net
Customer Success Manager	Contact details provided upon agreement of contract.	
Head of Digital Productivity	Contact details provided upon agreement of contract.	
TPHC Associate Director of DDaT	Contact details provided upon agreement of contract.	

Service desk management:



Section 6: Connect with us

Join the digital productivity revolution and learn more about the savings and gains your organisation can benefit from, only available through the TPHC Digital Productivity team.

Find out more about us and how the DPP could add value to your organisation:

www.transformationpartners.nhs.uk/digital-productivity
rf-tr.dpp@nhs.net

Appendix: Service catalogue

Clinical processes – primary care

The following lists provide high level details of the processes already built for various clinical teams, this list is not exhaustive. Each process is bespoke to suit each customer's operational requirements and the environmental variances.

System	Process name	Process description
EMIS	Filing lab results	Logs into EMIS Lab Reports and reads results. Files normal results and flags abnormal results for GP review
EMIS	Prescription confirmation text messaging	Downloads an EMIS report, logs into Accurx and sends the patient a text message
SystmOne	Sending Prescriptions to Community Pharmacies	Logs into SystmOne and sends SMS to each in scope patient to confirm the prescription has been signed and sent to their chosen pharmacy
EMIS	Fit Notes	Downloads a report, logs into EMIS, processes GP approved fit note and reason and sends SMS to patient
EMIS	Registering new patients with a GP	Reads eforms from dedicated inbox, validates fields, creates EMIS patient form and populates, sends a welcome SMS and acknowledgement email to the new patient
EMIS/SystmOne	Diabetes birthday bot	Reads Diabetes patient data and uses an algorithm to determine which tests require a review, sends a text message to invite patient to contact the practice for tests.

Clinical processes – secondary and community care

Team	Process name	Process description
Appointments	Appointments Disposal	Opens a manual report via the data warehouse, updates the Meditech appointment outcome and procedure code.
Appointments	Downloading Attend Anywhere usage reports	Logs into Attend Anywhere and runs and exports the consultation report to a shared drive.
Appointments	Medicines & Blood Discontinuation	Logs into Meditech, updates individual patient records discontinuing in scope orders.
Appointments	Outpatient Clinic Outcome Process	Logs into Allscripts and collects patient outcome, logs into Silverlink PAS and updates to DNA discharge/rebook or attended and creates a follow up appointment, generating a letter for each scenario.
Clinical reporting	Commissioner Portal Reports	Uploads reports into Umbraco and sorts each report on a daily process.
Clinical reporting	Departed Patients SystmOne	Logs into SystmOne and downloads the daily A&E type attendees/discharges for the multiple Urgent Treatment Centres and saves to share drive areas.
Medicines management	Pharmacy Homecare Invoicing	Opens a dedicated inbox, reads and validates invoice attachments, locates patient in Wellsky/JAC system and adds the invoice details.
PACS	Radiology Plainfilm Booking Process	Logs into CRIS, processes patients from the 'Request' worklist, opens the appointment diary, schedules the appointment within the diary, sends the letter to print via Envoy post and creates an output report.
Patient contact	Translation of texts for patient contact	Read emails in a dedicated inbox, bot translates into requested language and sends back to requestor.

PIMS (pre migration cleansing activity)	Waiting list with an Attended Appointment	Downloads the manual CSV report, logs into PIMS, searches for the patient record, opens the waiting list, cross checks and populates the required fields, confirms closure of the waiting list.
PIMS (pre migration cleansing activity)	Waiting list with Multiple Linked Appointments	Downloads the manual CSV report, logs into PIMS, searches for the referral and links to a newly created waiting list (WL) entry in PIMS and produces a management report.
Referrals	Estimated Due Date (EDD) from CRIS to K2	Opens CRIS report, logs into K2MS and updates patients' pregnancy profile with EDD.
Referrals	Antenatal self-referrals	Retrieves web form in a dedicated inbox, check for patient on Cerner and adds the referral, add details to Consent management system.
Referrals	Book Routine Referrals from eRS to Careflow Medway PAS	Logs into ERS and downloads the worklist, logs into Careflow and searches/register patient using SCR and updates referral details.
Referrals	Book routine referrals into PAS	Searches/creates patient record into a PAS and attaches to a waiting list.
Referrals	Careflow Discharge Planning	Extracts SQL data, logs into Careflow, searches/creates patient proforma and populates with complete discharge data set.
Referrals	Download attachments - various PAS	Logs into eRS, filters worklist, downloads the Clinical Information Summary and clinical attachments for UBRNs for specific specialities and uploads all the attachments as a single PDF file in the patient record on PAS.
Referrals	ERS to EPR - Download attachments, merge and upload into EPR	Identifies the in-scope referrals from the worklist on ERS, downloads the clinical information summary and

		any attachment(s), merges them into one document then uploads the merged document to the patients Powerchart - EPR record.
Referrals	Request received in CRIS	Logs into CrIS and specific worklist and process as request received, creates an outlook report and emails to team for manual activity.
Referrals	Update ERS with Triage Outcome	Using a manual Luna report, locates UBRN on ERS and completes the triage outcome and form comments, sends a patient SMS and/or GP email, where appropriate.
Waiting list	Modifying Clinician and Specialty with no future appointments	Opens a pre-downloaded file, logs into PIMS to edit clinician and/or specialty details on the waiting list episodes.
Waiting List	Modifying Clinician and Specialty with partial booking	Opens a pre-downloaded file, logs into PIMS to edit clinician and/or specialty details on the partial booking.

Recruitment automation service

HR Area	Title	Description	System access
Recruitment	ESR Trac Vacancy Link	Standalone process from advertising flow, takes an inscope list of adverts from Trac, creates in ESR and links back into Trac, allowing the applicant interface to work between the 2 systems for Offered Applicants	Trac & ESR
Recruitment	Trust ID invites	Initial invite is triggered by the sending of a Conditional Offer Letter in Trac, creating a guestlink and sending the Trust ID link and updating notes on Trac	Trac & Trust ID
Recruitment	Trust ID downloads of documents	A periodic check to download documents into an employee file and/or into Trac and update Trac notes	Trac & Trust ID
Recruitment	Trust ID chase responses	A periodic check to and chase for applicant responses in Trust ID and update Trac notes	Trac & Trust ID
Recruitment	Efolder Creation	Creates the applicant folder on a trust share area after a Conditional Offer Letter has been sent, triggered by an inscope list of applicants from Trac	Trac & ESR
Recruitment	Pre-Hire HPAN & Professional Registration Checks	Triggered after a Conditional Offer Letter has been sent using an inscope list of applicants from Trac. Checks the Professional Body website and screenshots findings, checks the HPAN website and screenshots findings, saving all back into an applicant folder and/or updating Trac status	Trac & professional body/HPAN websites
Recruitment	Eforms Downloading	Downloading either the Trac Onboarding Module forms or other eForms and saving into Trac or an efolder, added value options around onboarding for other depts such as security, IT, payroll, RA, etc	Trac & eform solution
Recruitment	Zip/Outcome File Downloads	Using an inscope Trac report, download applicant records into efolder/share drive area, can also include non-finalised records about to fall off the system	Trac
Recruitment	Pre-Hire updates into	Using Unique Identifiers to update Trac record with missing data e.g. NI, DOB,	Trac

	Trac	Prof reg	
Recruitment	Pre-Hire updates into ESR	Updating Unique Identifiers on ESR NI, DOB, NHS Net email, prof reg	Trac & ESR
Recruitment	Creating Missing ESR Applicant records	Fed from the Pre-hire Updates on ESR process where an applicant record cannot be found, once created loops into the Pre-Hire Update process	ESR
Recruitment	Pre-Hire IAT	Can include internal and external to support with bank transferring to substantive, L&D competencies held within other trusts for substantives, previous grade service for internal upgrades. Potential to trigger after Conditional offer Letter sent or further in the recruitment cycle depending on pay point confirmation or contract creation points	Trac & ESR
HR	Notifications to Manager and/or Employee	Right to Work, Maternity Returnees, Fixed Term Contracts Ending, Contract Amendment Letters	Trac & ESR BI & o365
Reporting	BI Reporting	Using Master Base Report to extract array of data and use the bot to filter, cut and save as the schedule requires	ESR BI & o365
Reporting	Recruitment Reporting	Using the suite of Trac downloads to feed into data warehouse, templates or dashboards to measure recruitment metrics	Trac

Non-clinical processes

This list details some of the processes built or designed for corporate teams. Whilst corporate teams may share common systems, they rarely have the same starting points or flows – each version is built bespoke to suit the customer's operational requirements.

HR Area	Title	Description	System access
Recruitment	Authorisation to hire	Receives the Vacancy Application Form (VAF) requests via email, adds these to the finance tracker, forwards the VAF to listed recipients for approval, checks for an approved VAFs, updates the tracker with details of each completed stage.	Outlook, Word
Recruitment	Advertising Jobs v1	Handles Outlook approved requests, verifies authorisation credentials, creates e-files on shared drive and a sequential ref number, populates Trac advert details and publishes. Creates requisition and vacancy in ESR and links back in Trac.	Trac & ESR
Recruitment	Advertising Jobs v2	Receives and logs vacancy request form from authorising managers via Outlook. Hands off to the recruitment team to link to an approved e-RAF form/pool who creates a job file and job reference as the trigger for the bot to create the ESR vacancy and requisition. Completes publishing of advert within Trac and NHS Jobs.	Trac & ESR
Recruitment	Advertising Jobs v3	Creates an ESR vacancy and requisition for all Trac vacancies. Once fully authorised, publishes for a period of days as a restricted advert, republishes time lapsed restricted adverts as public on Trac and NHS Jobs.	Trac & ESR
Recruitment	Redeployment administration	Checks live adverts for redeployment pool matching and creates clone adverts with comms to HR contact for the redeployee.	Trac
Recruitment	Shortlisting Notification (to managers)	Moves a closed Trac advert to shortlisting, checks for priority applicants (2 ticks) and redeployee matches and includes the detailed information in the template to the short listers for their next steps.	Trac

Recruitment HEE	Creates HEE applicants on Trac	Uploads in scope HEE applicants into a newly created vacancy.	Trac and master spreadsheet
Recruitment	Create applicant e-files v1	Create a job folder for in progress vacancies and creates a file for applicants in offer pending status.	Trac
Recruitment	Conditional Offer Letters – Pre-check Internal	Identifies in scope records, checks ESR/Trac data. If no ESR record found, updates applicant to External on Trac and follows External process. If ESR record found, follows Internal process.	Trac & ESR
Recruitment	Conditional Offer Letters - External	Identifies in scope, initiate Trac employment checks, create OH record, populate & send offer, send email notification.	Trac & ESR
Recruitment	Conditional Offer Letters – Internal	Identifies in scope records, retrieves ESR data, check ESR/Trac data, initiate Trac employment checks, creates OH record, populates and sends offer, sends email notification.	Trac & ESR
Recruitment	Create applicant e-files v2	Creates an applicant eFiles and subfolder hierarchy.	Trac, Network drives
Recruitment	Downloading new joiner forms	Downloads MS form and/or Trac onboarding forms into a shared area/applicant folder and uploads onto the applicant record.	Trac, MS Forms
Recruitment	Pre-Hire IATS	Initiates the Inter Authority Transfer (IAT) and downloads a copy to the applicant e-file.	ESR
Recruitment	ID Checks 1	Creates a userlink for applicants to return their ID documents and updates Trac.	Trust ID, Trac
Recruitment	ID Checks 2	Chases for outstanding ID checks.	Trust ID, Trac
Recruitment	ID Checks 3	Downloads returned ID documents and uploads into Trac. Checks and deletes duplicate links.	Trust ID, Trac
Recruitment	Applicant Zip Files 1	Downloads the finalised Trac record into an applicant e-file.	Trac
Recruitment	Applicant Zip Files 2	Catch all process - downloads the Trac record regardless of status into an applicant e-file.	Trac

Recruitment	ESR New Hires	Hires an applicant in ESR and updates their personal and contractual information.	Trac & ESR
Recruitment	Bank rehires via applicant records	Creates an ESR applicant record for substantive leavers remaining on the internal bank. A subset of substantive personal and pre-employment check data is updated into the new record.	ESR
Recruitment	Professional Registration checks	Runs, downloads, and filters a report from Trac and checks the HPAN and appropriate professional registration websites for NMC, HCPC, GMC, GMC, GOC, GPhC, Social Work England registered applicants.	Trac, HPAN, Professional registration websites
Recruitment	Recruitment satisfaction survey	Collects in scope records from Trac, searches applicant, sends survey monkey via Trac, sends management report.	Trac, Survey Monkey
HR Onboarding	Totara (LMS) onboarding	Downloads a Trac report, creates a new starter record in the learning system and send details to new starter.	Totara
HR Onboarding	Self-service for new starters	Downloads a new starter report, sends ESR login details and flags missing emails to line managers.	ESR
HR	Rotation position changes	Updates ESR with the new position and fixed term end dates.	ESR
HR	Appraisals compliance reminder	Downloads the report worklist and sends an email notification to the employees' manager, reminding them to complete overdue appraisal.	ESR
HR	Appraisal input	Accesses an e-form, populates ESR screens with required information, creates an output report.	ESR, Office365
HR	Amendment to contract letters	Accesses a pre-filtered BI Change event log, creates a personalised letter and sends as PDF attachment to the employee email.	Excel, Outlook, Adobe
HR	Certificate of Employment Letters	Populates a template based on an e-form submitted by the employee with a tick list of data items required for their request.	eForm feed, Excel, Word and Outlook
HR	NHS.net email addresses to	Downloads a change event log report, finds the employee record on ESR and relinks employee record to the	ESR

	ESR	username.	
HR	Fixed term end dates - manager notifications	Downloads a staff list focussing on fixed term end dates within x months, sends a reminder email of next actions to the managers of those due to end.	ESR, Outlook, Excel
HR	Maternity returnee - manager notifications	Downloads a staff list focussing on maternity returnees within x months, sends a reminder email of next actions to the managers of those due to return.	ESR, Outlook, Excel
HR	Right to Work - employee notifications	Downloads a staff list focussing on those with right to work expiry dates approaching within x months, sends a reminder email of next actions to the affected employees.	ESR, Outlook, Excel
HR	Reference Requests v1	Filters Outlook to look for Trac reference requests, accesses SQL database of workforce information to derive information, populates the Trac template and returns to requestor.	Outlook, SQL tables
HR	Reference Requests v2	Filters Outlook to look for Trac reference requests, accesses ESR BI Staff List and Leavers reports to identify employee record, runs the ESR BI Standard reference and accesses ER database to add additional fields, returns saved report to requestor.	Outlook, ESR, Selenity
HR business intelligence	ESR BI Reporting	Various reporting from ESR with output reports saved to different drives and folders and formats based on frequency, filters and effective dates that are controlled by the end user team.	ESR
IT	New Starter IT	Downloads Trac start date booked report, checks for current windows account, checks for NHSmail, creates windows account, creates/assigns NHSmail, links to network drive, emails line manager, creates business report, updates audit file.	ESR
Finance	Invoice management	Reads dedicated inbox, forwards any non-invoice emails onwards, validates invoices and sends to scan station	Outlook
Finance	Emailing PO Receipting Reminders	Logs into NEP, downloads the open PO report and emails the assigned contacts with PO details.	NEP, Outlook, Excel
Finance	Emailing Debt	Logs into NEP, downloads aged debt	NEP, Excel,

	Reminder Letters	report and outstanding debt report, compares against previous month debt report for those still outstanding, separates into excel sheets per customer and email sheets to customer.	Outlook
--	------------------	---	---------