Service Catalogue

V1.1

Last updated: 01/05/2024

Your Trusted IT Delivery Partner
Our Services

IT Operations

We pride ourselves on delivering an exceptionally **high standard** service while being **responsive** and **customer-centric**.

Project Management

Our comprehensive project and programme management service drives **business change** and the fulfilment of your **strategy**

Digital Strategy

We are all continually reviewing the way we work and with **Digital** becoming the new norm, we can help with your digital journey.

IT Infrastructure

We provide **robust** and **responsive** Infrastructure services, and a **proactive** approach to managing cyber security.

Information Governance

Our **experienced** and qualified **experts** provide advice and guidance on **Information Governance**, **RA** and **Clinical Safety**.

IT Training

We work closely with you to deliver training that is **designed** and **tailored** to your requirements and delivered **flexibly**.

Development

We **design**, **develop** and **host** websites, intranets, mobile apps and web applications designed to **meet** your requirements.

VoIP, Mobiles & Connectivity

Fixed cost mobile plans and cloud hosted VoIP. **Fully scalable** from single users to multi-site call centres.

Digitalisation & Print

Print and digital solutions, helping you **work smarter, reduce costs, automate** your working processes and **improve efficiency.**

Learn more about our services n3i.co.uk/services

Available Services

Service Name	Service Ref	Notes
IT Operations : Service Desk Support 1.1		
Service Desk	1.1.1	
Out of Hours Support	1.1.5	
Account Administration	1.1.6	
IT Infrastructure : General Infrastructure Services 1.2		
Active Directory	1.2.1	
Data Storage	1.2.2	
Network Printing	1.2.3	
Backup and Restore	1.2.4	
Application Hosting	1.2.5	
Monitoring	1.2.6	
Remote Access	1.2.7	
LAN/WAN Network Services	1.2.8	
Wireless Services	1.2.9	
Telephony Service	1.2.10	
Office 365	1.2.11	
IT Operations : Desktop Support Service 1.3		
General Desktop Support Services	1.3.1	
Computers / Workstation	1.3.2	
Peripheral Equipment Management	1.3.3	
IT Infrastructure : Disaster Recovery and Business Continuity 1.4		
IT Delivery Partner Disaster Recovery (DR) and Business Continuity (BC)	1.4.1	
Business Continuity Support Services	1.4.2	
IT Infrastructure : Asset Management and Software Licensing Service 1.5		
Assets - Hardware	1.5.1	
Disposal of Equipment	1.5.2	
Software Licensing management and support	1.5.3	
IT Infrastructure : Cyber Security 1.6		
Cyber Security Service Delivery	1.6.1	
Cyber Security Monitoring & Reporting	1.6.3	
Cyber Security CareCERT	1.6.4	
Cyber Security Strategy & Advice	1.6.5	
Cyber Security Incident Management	1.6.6	
Cyber Security Supporting Projects	1.6.7	

Information Governance : General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 1.7		
GDPR Compliance	1.7.1	
IT Procurement Service : Ordering, Advice and Guidance 2.1		
IT Procurement Service Ordering of IT Equipment	2.1.3	
IT Procurement Service Advice & Guidance	2.1.4	
IT Programmes : Technology Infrastructure Refresh Service - 3.1		
GP IT Hardware Refresh Service	3.1.1	
IT Programmes : Training Service 4.1		
Training Services	4.1.1	
IT Programmes : Project and Change Management Service - 5.1		
Project and Programme Management		
IT Operations : Customer Relationship Management - 6.1		
Customer Liaison Management	6.1.1	
IT Programmes : Digital Solutions - 7.1		
Digital Solutions – Development Services	7.1.1	
IT Infrastructure : Estates Strategy Service 8.1		
Estates Premise IT	8.1.1	
Registration Authority – 9.1		
Support of Smartcards	9.1.1	
Maintenance of Registration Authority Service (RA)	9.1.2	
RA Training	9.1.3	
RA Reporting	9.1.4	
IT Operations : NHSMail (Email Service) 10.1.1		
NHSMail Provision of Accounts	10.1.1	
NHSMail Maintenance and Support	10.1.2	
Information Governance : Information Governance 11.1		
Incident management & investigations	11.1.1	
IG Advice and Support	11.1.2	
Information Governance : Clinical Safety Assurance - 12.1		
Clinical Safety Assurance Advice & Guidance	12.1.1	
Digital Transformation Service - 13.1		
DTS Programme Management	13.1.1	
DTS Project Delivery	13.1.2	
DTS Horizon Scanning	13.1.3	
DTS Customer Engagement	13.1.4	

SCHEDULE A – Service Description

Service Name	Service Ref	Service Description	Customer Responsibility	Additional Services not funded in main SLA
IT Operations : Service Desk Support 1.1				
Service Desk	1.1.1	The N3i Service Desk provides a single point of contact (SPOC) for all IT incidents and service requests. • a single telephone number; • single email address; • self-service portal A single ticket will be allocated for the duration of a request. N3i will provide the ability to re-open a request should the user not be satisfied with the proposed resolution implemented to close the incident / request. Our Core Service Desk Hours: - Monday – Friday: 08:00 – 18:30 The N3i Service Desk will attempt to resolve all calls on initial contact. This will involve resetting all passwords; securely remotely accessing PCs to resolve incidents and providing advice to the user when required. The N3i Service Desk will ensure the user is provided with a summary of incident / request fulfilment following completion of support provided.	Report all IT incidents and requests for change to the IT service desk by telephone, email, or web interface. Provide the N3i service desk with required information to allow the correct recording of incident or request. Allow N3i staff reasonable access to premises or access to IT equipment via remote control to allow incident resolution to take place. When escalating logged incidents, provide the incident reference number. Ensure staff take appropriate action when advised of IT service downtime	Out of Hours Support
Out of Hours Support	1.1.5	Provide Out of Hours IT Support for systems/services that are high priority (P1/P2 incidents) to the customers		
Account Administration	1.1.6	Provide active directory account administration service which includes the creation, amendment, deletion, and auditing of all user accounts. This service ensures only fully authorised users are allowed access to the Network by checking the appropriate approval has been received for each request. Carry out monthly audits to ensure only appropriate users are active (non-active users defined as no access within 3 months) on the network.	Ensure internal processes (e.g., starter / leaver management) are in place so that only authorised users are granted access to the agreed resources.	Out of Hours Support

IT Infrastructure : General Infrastructure Services 1.2				
Active Directory	1.2.1	Provision of Active Directory services to allow access to desktop and server resources. All users will be provided with a unique Active Directory account on a suitable domain. Any planned downtime is to take place outside of core hours. N3i will liaise with the customer to agree the process and communications for any planned downtime, the expectation that a minimum 48 hours' notice will be provided - in exceptional circumstances the notice period may be reviewed.	Ensure internal processes agreed with N3i are in place so that only authorised users are granted access to the agreed resources.	Out of Hours Support
Data Storage	1.2.2	Provision and management of sufficient secure on premise or secure cloud storage to host the customer's data including archived email. Any planned downtime is to take place outside of core hours. N3i will liaise with the relevant customer(s) to agree the process and communications for any planned downtime, the expectation that a minimum 48 hours' notice will be provided - in exceptional circumstances the notice period may be reviewed.	To ensure that stored data is appropriate and relevant for business use only.	Out of Hours Support
Network Printing	1.2.3	The ability to host and manage print queues (either on premise or secure hosted) for customer printers. Liaison with 3rd party print solution providers.	Third parties must adhere to security standards	
Backup and Restore	1.2.4	All customer data saved to a network drive will be backed up to an offsite location on a regular basis defined as: • Daily Backups to a secure repository. • Full weekly backups must be maintained for 28 days and offsite (or duplicate data centre) backups for 1 year. Restores to be requested through the IT Service Desk and incident/request categorisation will apply.	Ensure that all requests for restore of data are completed within timescales consistent with retention and recovery times. Backup of data held on local desktop or mobile devices.	Office 365 Backups
Application Hosting	1.2.5	By agreement with the **Customer**, hosting of server-based specialist applications. Liaison with 3rd party providers to define, implement maintain appropriate server provision or network access including, where agreed with the **Customer**, support for 3rd party remote access solutions to enable remote management of systems or application.	Provision of sufficient resource to host applications May be subject to agreement to any additional costs for specific hardware	For 3rd party applications ensure required software application licences and support are purchased

Monitoring	1.2.6	Proactive monitoring and alerting of all relevant infrastructure including server, storage, and network resources to anticipate and prevent IT incidents ensuring maximum availability. N3i will put in place 24-hour monitoring and alerting system which allows for notification of unexpected / unscheduled system downtime.		
Remote Access	1.2.7	The provision and support of a secure remote access solution to provide access to hosted systems and local network or cloud service resources.		
LAN/WAN Network Services	1.2.8	Provision of management, support, and where appropriate configuration, of: • HSCN connections to main and branch practice sites as per national entitlement and local determination. • Wide Area Network / Private Network / Community of Interest Network (COIN) utilising shared connectivity with other partners wherever practicable and cost effective. • Filtered and managed Internet connections to all sites (where not provided through HSCN gateway) or support/management of internet access though liaison with HSCN service provider. Support active network devices (e.g., switches routers etc.) including configuration and deployment management on managed IT equipment.	Allow N3i staff reasonable access to premises or access to IT equipment Provide clear access, safe working, and adequate power provision to network communications cabinet.	Out of Hours Support
Wireless Services	1.2.9	A Wi-Fi service for customer sites for a range of service set identifiers (SSIDs) including but not limited to N3i, NHS Wi-Fi, GovRoam.	A Wi-Fi service for each Place and practice meeting the NHS Wi-Fi Technical & Security Policies and Guidelines https://digital.nhs.uk/nhs-wi-fi/GP-practices	
Telephony Service	1.2.10	Provision, maintenance and technical support of the necessary infrastructure to support existing and new phone systems		
Office 365	1.2.11	Provision of one email account per individual on request. Provision of shared / generic email accounts on request. The on-going maintenance of email accounts, which includes the moving and deleting of accounts, password resets and unlocking accounts	Email service provided via NHSMail platform.	Microsoft 365 Licensing purchases

IT Operations : Desktop Support Service 1.3				
General Desktop Support Services	1.3.1	Provision of second- and third-line break/fix technical support for desktop hardware, software, and peripherals. Provision of planning and implementation services for requested installations and moves, together with asset management, configuration management and documentation of desktop assets. Support is undertaken via remote and onsite activities and adheres to agreed service level agreements. Provision of anti-virus, malware protection, encryption, and access management service Liaison with core system suppliers for management of on-going system updates, as necessary.	Allow IT Delivery Partner informatics staff reasonable access to premises or access to IT equipment via remote control to allow incident resolution to take place. **Customer** is responsible for the physical security, PAT testing and power supply for IT equipment **Customer** is responsible for the hardware assets including refresh and must ensure they support national NHS mandates such as Windows 10 and devices are in warranty.	Out of Hours Support Support for applications and IT hardware devices not specified in this SLA
Computers / Workstation	1.3.2	Installation and support of all **customer** provided computers, laptops and other mobile computing devices, and peripheral equipment, meeting security standards and compatibility constraints such as mobile device management, encryption, remote lock, remote wipe, etc. Installation and support of all standard software and applications. Support for the assessment (including compatibility and security considerations) and, where agreed by the **customer**, installation of additional software. Emergency equipment procured by the **customer** will be maintained and held in the event of network failure e.g., spare laptops, printers, scanners etc. Maintenance of adequate stock levels of replacement equipment and spare parts to support agreed incident resolution times. The user workstations are locked down and managed via active directory group policies. Users are not able to install software or change critical settings. Produce and Maintain Standard Operating Procedures (SOP). Keep customer informed and updated on progress of related incident	Allow N3i staff reasonable access to premises or access to IT equipment via remote control to allow incident resolution to take place. Agree with N3i the core hardware and software through Warranted "supported" Environment Specification" - updated at least on annual basis. Costs for repair of hardware outside warranty period or not covered by warranty.	Out of Hours Support

		Defined and documented standardised desktop image(s) to included contact details (web-portal; phone; e-mail) for Service Desk Support and any urgent service information, with a formal change control management system.		
Peripheral Equipment Management	1.3.3	Deploy and maintain other hardware, for example including but not limited to check-in kiosks, call screens, scanners, smartcard readers, barcode readers, printers including dual bin feed printers for consulting rooms and MFDs, where necessary. Where the installed & supported equipment is covered by a warranty, the IT Delivery Partner will engage with the manufacturer's support services to arrange repair or replacement, where necessary. Liaison with 3rd party hardware providers (e.g., managed print solutions, clinical systems etc.) where required for specification, installation, and support	Consumables are the responsibility of the customer.	
IT Infrastructure : Disaster Recovery and Business Continuity 1.4				
IT Delivery Partner Disaster Recovery (DR) and Business Continuity (BC)	1.4.1	**Business Continuity requirements** N3i will ensure all data changes over a 24-hour period will be backed up and stored off site. Note enhanced data backup services where provided will allow more frequent backup schedules. Maintain system status information with alerts for critical downtime/failures ensuring this reflects 100% of known issues and is not more than one working hour out subject to 3rd party provider information. For business-critical incidents (priority level 1) a Lessons Learned Report (with relevant action plan as appropriate) to be provided to customer within 2 weeks of the recorded resolution of the incident on the service desk **Business Continuity and Disaster Recovery plan and arrangements** N3i is required to maintain an annually reviewed business continuity plan and validated IT disaster recovery plan for services provided within this specification. The plans are to be submitted to customer annually by 1 April of each year. In the event of a major event when the plan is utilised this will trigger a review of the plan and reset the 12-month review period. The Business Continuity plan will include continuity plans in response to threats to data security, including significant breaches or near misses		

Business Continuity Support Services	1.4.2	Provision of IT advice and guidance in relation to IT to support the development of customer business continuity plans.	Develop and maintain business continuity plans.	
IT Infrastructure : Asset Management and Software Licensing Service 1.5				
Assets - Hardware	1.5.1	100% of assets will be maintained via an electronic Configuration Management Database (CMDB). All assets (devices or systems purchased by **Customer**) will be provisioned with a unique asset tag and recorded in the CMDB. To note - any assets purchased by the **Customer** through N3I should be separately identified and recorded on the asset register. The lifecycle of any asset can be reported on via the electronic CMDB at any time.	Provide N3I with information relating to any hardware move, additions or deletions. **Customer** is responsible for the hardware assets and software licenses including refresh and must ensure they support national NHS mandates such as Windows 10 and devices are in warranty.	
Disposal of Equipment	1.5.2	As agreed with the customer all assets will be disposed of via an authorised supplier and will be destroyed in line with EU and National Regulations and The Waste Electrical & Electronic Equipment Directive (WEEE), detailed records and certificates will be provided by the authorised supplier. Detailed records of all disposals will be maintained and authorised by senior personnel and the electronic CMDB will be updated accordingly when items are disposed of. All hard drives will be removed prior to disposal and securely destroyed with an audit trail maintained.	EU and National Regulations and The Waste Electrical & Electronic Equipment Directive (WEEE).	
Software Licensing management and support	1.5.3	100% of IT software assets regardless of ownership used on N3i supported devices will be recorded via an electronic Configuration Management Database (CMDB). All software required for the provision of IT services will be maintained by N3i.	Provide software licence and national contract management support to the customer (ensuring licensing, legal compliance, and national contract management)	
IT Infrastructure : Cyber Security 1.6				
Cyber Security Service Delivery	1.6.1	Ensure that all ICT services are delivered in accordance with current and future NHS Digital CareCERT recommendations including • Risk Assessment • Risk Management • Security Architecture	Ensure that all staff receive regular training on Information governance and Information Security. Maintain and update acceptable use policies	Additional ad hoc costs for major incident support out of hours to be agreed with the customer. Out of Hours Support

		• Audit and Review • Incident Management • Penetration Testing • Cyber Incidents response • Vulnerability assessments Vulnerability and, where indicated Penetration, tests will be conducted at an agreed frequency not less than once per annum with outcomes and required actions shared with the customer subject to maintaining security of findings. Security incident response should include out of hours response and onsite support where required		
Cyber Security Monitoring & Reporting	1.6.3	Monitor security threats to IT systems and networks, through deployment of defence and incident management, to include: • Access control; • Application control; • Asset Management; • Boundary protection; • Device Encryption (and remote lock/wipe of mobile devices); • Hardware & software management including patching and upgrade; • Network security; • Vulnerability assessment.	Acceptance that ability to deploy recommended upgrades may be limited by system/application supplier constraints.	Out of Hours Support
Cyber Security CareCERT	1.6.4	Provide information security consultancy and help with security issues in system design and development. Provide guidance and advice to support staff education and awareness. NHS Digital CareCERT advisories must be acted on in line with suggested timescales, and evidence through CareCERT Collect.		Out of Hours Support
Cyber Security Strategy & Advice	1.6.5	Cyber Security Advice to be available to customer on: • Cyber security audits; • Cyber security investigations; • Specialist (IT Security).		Out of Hours Support
Cyber Security Incident Management	1.6.6	Advice and support for the customer on incident assessment, reporting and management in accordance with national guidance and legal requirements. To include:		Out of Hours Support

		• Advice on post-incident reviews and recommended actions for practice implementation; • Leading or directing incident reviews and investigations where highly specialist knowledge is required, or complex multi-party issues are involved;		
Cyber Security Supporting Projects	1.6.7	Advice for customer and the appointed project teams on Cyber Security where projects involve (but not limited to): • New technology and system procurements; • Deploying new technologies and devices; Support for projects beyond general advice for example preparing Cyber Risk Assessments should be resourced as part of the project plan.		Out of Hours Support
Information Governance : General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 1.7				
GDPR Compliance	1.7.1	Provide support, advice and guidance to the customer around GDPR:- • Ensure that they are GDPR (EU) 2016/679 and Data Protection Act 2018 compliant; • Ensure that any data processor or data controller responsibilities are fully documented and agreed with the customer; • Assure the commissioner and provide evidence when asked that the providers and their 3rd party contractors are compliant for keeping the services provided to the commissioner GDPR and Data Protection Act 2018 compliant, included in this would be advice on what action the commissioner will need to take on services/systems to ensure compliance; • Assist the customer in the investigation of possible and actual information security breaches and incidents including evidence to support post-incident reviews and actions for customer implementation. Ensure that a Data Protection Impact Assessment is undertaken covering the service provision, with outcomes and recommendations shared with the customer.		Out of Hours Support
IT Procurement Service : Ordering, Advice and Guidance 2.1				
IT Procurement Service Ordering of IT Equipment	2.1.3	Procure and order all IT equipment and software as agreed with the customer, if NHS customer to be in line with the current GPIT operating model and against appropriate SFI’s. N3i will undertake an annual review of the IT hardware catalogue with an identified group of customer stakeholders.		

		N3i will offer the ability for the customer to procure IT hardware / software - which should be available via a catalogue ordering process.		
IT Procurement Service Advice & Guidance	2.1.4	Providing advice and guidance on the procurement of new IT solutions to ensure compatibility with, and compliance to, NHS standards.	Customer to purchase new hardware through the N3i service Desk procurement service, for any new starters/service. Customer responsible for hardware Refresh as per Schedule B – Managed Assets.	Out of Hours Support
IT Programmes : Technology Infrastructure Refresh Service - 3.1				
GP IT Hardware Refresh Service	3.1.1	Provide and deliver a refresh programme that will identify and replace GP IT hardware where it has reached its service life change date, as a minimum every 4 years, subject to NHS England guidance and funding, including assessment, rollout and disposal	Allow N3i staff reasonable access to premises.	
IT Programmes : Training Service 4.1				
Training Services	4.1.1	Provide the customer access to training which will include training for: • GPSoC/GPIT Futures core clinical systems; • National digital systems e.g. SCR, EPS2, ERS. And will include training requirements arising from: • Migration; • Mergers; • New Functionality (e.g. upgrades or new clinical systems); • Staff turnover; • Refresher training; • Support practice optimisation of principle GP clinical systems and national digital systems; • Microsoft Office Suite (Office 365) Service will be delivered through the following methods e.g. face- to-face, online	Training for customer purchased systems e.g. Sage Accounting, clinical devices, business administration and office systems.	Additional Service on demand

IT Programmes : Project and Change Management Service - 5.1				
Project and Programme Management		Provide Programme and Project management resources as commissioned by the customer to include: • Production and maintenance of programme plans and documentation including Project Initiation Document, Business Case), highlight reports, exception reports, risk and issue logs, etc.; • Change Management; • Stakeholder analysis, engagement and communication; • Working within agreed governance and accountability; • Standalone risk and issue management, using a structured risk • management approach such as MoR; • Benefits using an established evaluation process; • Standalone Supplier Management/Liaison within an outsourced customer-lead project or programme to maximise N3i's efficiency, quality and value for money. • Delivery of Projects should be fulfilled, where possible, using existing resources on a service priority basis.	Nomination of Senior Risk Owners and governance boards as appropriate.	Resourcing of large complex projects, will be discussed on a case by case basis
IT Operations : Customer Relationship Management - 6.1				
Customer Liaison Management	6.1.1	Provision of a named manager as contract manager. Management of complaints and issues from customers in accordance with agreed procedure. Provision of service performance reports e.g. incident closure customer survey (quarterly reports) and customer satisfaction survey (no less than once a year), with timings to be agreed. Support the customer in the management and advice in relation to IT provision and development. Including provision of best practice advice and guidance relating to all aspects of the IT service provision and delivery.		
IT Programmes : Digital Solutions - 7.1				
Digital Solutions – Development Services	7.1.1	Develop, host, maintain and support web applications including content management systems, public and private websites. Hosting (including secure hosting), configuration and monitoring of web servers.	Administration of website content and access	Out of Hours Support

IT Infrastructure : Estates Strategy Service 8.1				
Estates Premise IT	8.1.1	Provision of advice and guidance to support the development estate relevant to the provision of IT services and systems. Advice, assessment and compliance and support, including deployment of IT infrastructure and Desktop kit and IT kit in customer estate.		Out of Hours Support
Registration Authority – 9.1				
Support of Smartcards	9.1.1	Our Core RA Support Hours: - Monday – Friday: 09:00 – 17:00 Delivery of service including configuration, issuing and management of smartcards (provision for new starters and removal of roles for leavers). The Registration Authority (RA) Service will operate within National Guidelines and polices. The RA Service ensures users are registered to e-gif level 3 standards are given appropriate access rights for their job role for use with relevant Smartcard applications within agreed service level agreements. Assurance of the customer adherence to RA Policy and processes. If assurance cannot be obtained, then the issue should be escalated as appropriate.	The customer must have its own ODS code, setup by NHS Digital and meeting the standards met in the Data Protection Security Toolkit The customer will need to ensure that their own infrastructure allows them access to the NHS Spine.	Out of Hours Support Setting up new workgroups, New organisations (ODS)
Maintenance of Registration Authority Service (RA)	9.1.2	Acting within RA Guidelines Smartcard Management will include the following: • General RA Troubleshooting and call escalation to NHS Digital • Re-issue Smartcards, as appropriate. • Promoting self-service. Sponsors of customer will typically perform the roles below however the IT Delivery Partner may need to provide support where required: • Add / Remove roles. • Amending Positions. • Unlocking / Reset PIN. • Renew Certificates. Provide the customer with a facility to notify the RA team when staff leave the practice or no longer require RA access, and ensure access is removed within the relevant priority for user account management (National Data Guardian standard 4 - Data Security and Protection Toolkit).	The customer must have its own ODS code, setup by NHS Digital and meeting the standards met in the Data Protection Security Toolkit The customer will need to ensure that their own infrastructure allows them access to the NHS Spine.	Out of Hours Support

RA Training	9.1.3	The RA Service provides end users with training in the appropriate use of their Smartcard. Training and advice will be given to Sponsors dealing with RA issues on-site and in the use of CIS. Documentation is also provided to sponsors following all training.		Out of Hours Support
RA Reporting	9.1.4	The provision of audit reports to be undertaken to assure smartcard compliance and appropriate access is adhered to and Cyber Security and Data Security and Protection requirements have been met. Support for ad-hoc investigations.		Out of Hours Support
IT Operations : NHSMail (Email Service) 10.1.1				
NHSMail Provision of Accounts	10.1.1	Delivery of service in accordance with national standards and service level agreements. Provision of one NHSMail account per individual on request. Provision of shared / generic NHSMail accounts on request.	The customer must have its own ODS code, setup by NHS Digital and meeting the standards met in the Data Protection Security Toolkit Timely notification of starters and leavers within organisation	Out of Hours Support Office 365 Licenses Office 365 Backups
NHSMail Maintenance and Support	10.1.2	The on-going maintenance of NHSMail accounts, which includes the moving and deleting of accounts, password resets and unlocking accounts. Escalate to the national NHSMail Helpdesk should it require further attention. This support includes the connection of accounts to Microsoft Outlook when connected to the core network. Provide the customer with a facility to notify the IT Delivery Partner when staff leave the practice or no longer require NHS mail access, and ensure access is removed within the agreed priority for user account management (National Data Guardian Standard 4 - Data Security and Protection Toolkit)	Timely notification of changes required within organisation. Where available the customer will use self-service.	Out of Hours Support Office 365 Licenses
Information Governance : Information Governance 11.1				
Incident management & investigations	11.1.1	Delivery of IG service which includes: • Compliance advice and IG Support for the customer;		Out of Hours Support

		• Support the customer in the reporting and management of incidents; Liaison with the customer nominated and / or ICB Data Protection Officer (DPO); • Supporting cyber related Incident management and reporting. • Provision of advice and/or support the customer on the investigation of possible information security breaches and incidents. • Advising on incident assessment (dependent upon severity of incident). • Advice on post-incident reviews and actions for customer implementation. • Provision of advice and/or support to the customer on the investigation of possible information security breaches and incidents in practices. Advice on post-incident reviews and actions for customer implementation.		
IG Advice and Support	11.1.2	A review at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. This may for example be a facilitated workshop at board level which would encourage shared learning (National Data Guardian Standard 5 - Data Security and Protection Toolkit). Advice to support Practices develop and maintain best practice processes that comply with national guidance on citizen identity verification, including “Patient Online Services in Primary Care – Good Practice Guidance on Identity Verification”, that underpins the delivery of patient facing services, and assurance requirements as these are developed. Data Protection Officer (DPO) Resource A Data Protection Officer function will be available to support the customer, as required. The service will include: • Access for the customer between 08:00-18:30 Monday to Friday, to specialist qualified advice on GDPR matters. • Advice on compliance with GDPR obligations, including those outlined in paragraph 1 of Figure 7 in this document • Advice reflecting national guidance on GDPR compliance as it is published. The primary role of the Data Protection Officer (DPO) will ensure that practices will process the personal data of its staff, patients, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.		Out of Hours Support

		Advice to support the customer with compliance with the National Data Guardian eight-point data sharing opt-out model. All published CareCERT Best Practice and NHS Digital Good Practice Guides will be reviewed and where applicable incorporated into GP IT Services. The service should work closely with the commissioned GP IT Security (Cyber Security) Service.		
Information Governance : Clinical Safety Assurance - 12.1				
Clinical Safety Assurance Advice & Guidance	12.1.1	A comprehensive clinical safety assurance service, ensuring that providing the necessary advice and guidance is given relevant to national requirements for management of clinical risk in relation to the deployment and use of health software		Out of Hours Support