BCPCouncil.gov.uk

Information Technology & Information Services

IT TECHNICAL STRATEGY AND STANDARDS

Document Version Control

Version	Revision Date	Summary of changes	Author
v0.1	28/01/2020	Initial Draft	Marc Biondic, IT Infrastructure Manager
v0.2	29/01/2020	Second Draft	Marc Biondic, IT Infrastructure Manager
v0.3	30/01/2020	Technical Peer Review	Marc Biondic, IT Infrastructure Manager
v0.4	13/02/2020	Management Peer Review	Marc Biondic, IT Infrastructure Manager
v0.5	27/05/2020	Section 10.0 Updates	Marc Biondic, IT Infrastructure Manager
v1.1	08/07/2020	Data Extraction and API section added	Marc Biondic, IT Infrastructure Manager
v1.2	29/07/2020	Updated Purpose and Background	Marc Biondic, IT Infrastructure Manager
v1.3	01/09/2020	Agreed at CMB	Marc Biondic, IT Infrastructure Manager

Table of Contents

Document Version Control 2
1.0 Purpose and Background 3
2.0 IT Technical Strategy 4
3.0 IT Server & End-User Device Platforms 5
4.0 Virtualisation 6
5.0 Databases 6
6.0 Data 6
7.0 Security 8
8.0 Authentication and Authorisation 8
9.0 Remote Access 9
10.0 Networks & Communications 9
11.0 Green IT 9
12.0 Documentation 10
13.0 Service Management Expectations 10
APPENDIX A: Borough of Poole Legacy IT Infrastructure 11
APPENDIX B: Bournemouth Borough Council Legacy IT Infrastructure 15
APPENDIX C: Christchurch Borough Council Legacy IT Infrastructure 19
APPENDIX D: M365 within BCP Council 22

1.0 Purpose and Background

1.1 The purpose of this document is to set out the IT Technical Strategy and technology standards adopted by BCP Council. Appendices provide extra detail about core IT infrastructure currently in use. It should be in the context of the following strategies (note: some still under development).

1.2 BCP Council's Corporate Strategy can be found online here.

1.3 This IT Technical Strategy supports the delivery of the Organisational Development plan, which can be found here. From this plan there are key statements and prospective IT solution providers should detail how their proposals help the council meet its strategic objectives. These include, but are not limited to:

1.3.1 All of our services, whether "front" or "back" office, will be technology enabled and supported in a way that is consistent with a 21st Century organisation. Our way of working will support the work being done wherever, however, and whenever is optimal.

1.3.2 The proposed Operating Model allows significant reduction in our ICT Enterprise Architecture by focussing our relationships on a small number of more strategic technology relationships within different parts of the model, e.g. single technology platform for the "front door" and the same for the enabling/back office functions.

1.3.3 We will use data alongside strong relationships with key external stakeholders to create an entirely new and enhanced level of understanding of our communities and their needs.

1.3.4 We will use the process of delivering this transformational change to ensure our commitment to the Council's pledge to become Carbon Neutral by 2030.

1.4 The IT Technical Strategy supports the delivery of BCP Councils Digital Strategy. This aims to create a digital environment and Services that are so good they are used as first choice by most people and are easy to use. It is delivered through 4 sections:

1.4.1 *Digital Workplace: We will enhance our capacity and capability by using digital design and emerging technology to collaborate effectively, innovate and make informed, transparent decisions.*

1.4.2 *Digital Services: We will take every opportunity to digitally transform services to reflect our new operating model whilst ensuring we meet the needs of our communities and provide a great online user experience that is aligned to our Customer Access Strategy.*

1.4.3 *Digital Place: We will continue to build on the successes of the transforming cities fund and smart cities activity to improve connectivity, enhance economic growth, improve the quality of life and opportunities for innovation in our area.*

1.4.4 *Data, Insight and Collaboration: We will use, rationalise, manage and exploit the data we have. We will use analytics and data science to provide us with insight to support informed decision making, service design and collaboration.*

1.5 The Customer Access Strategy is currently under development. This Technical Strategy will be reviewed alongside the emerging Customer Access Strategy to ensure there is continued alignment.

1.6 This document will be updated annually, or as significant IT technical changes are implemented.

2.0 IT Technical Strategy

2.1 In support of the Organisational Development Plan and Digital Strategy, BCP Council's IT Technical Strategy can, at a high level, be summarised as "Cloud First" and "Digital by Default".

2.2 The IT Technical Strategy will, over time, enable BCP Council to reduce its IT capital expenditure by dramatically reducing the complexity and sprawl of IT software, platforms, and infrastructure across the business.

2.3 BCP Council will seek to partner with a minimal number of IT service providers who can provide premium services at a reasonable cost.

2.4 BCP Council has growing footprints in the Microsoft365 (M365) platform, including a Council wide deployment of Office365, and the Microsoft Azure platform as well as a growing set of business process solutions within the Dynamics365 space.

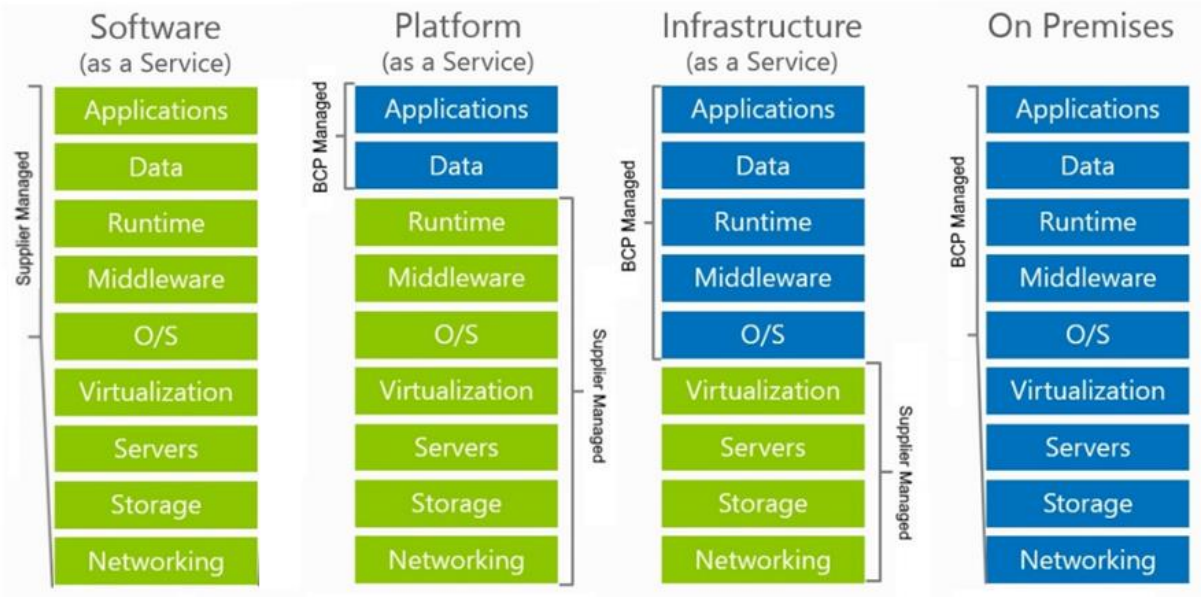
2.5 BCP Council will have a preference to implement Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) solutions over and above on-premise solutions (i.e. hosted within BCP Councils datacentre).

2.6 BCP Council will have a preference to implement solutions that are delivered via the M365 or Dynamics365 platform AND meet the functional requirements of BCP Council.

2.7 At a high level, Appendix D articulates the lengths to which BCP Council is seeking to leverage its investment in the Microsoft toolsets to deliver the IT Technical Strategy and details some of the work currently underway or about to start.

2.8 For the purpose of clarity, BCP Councils definitions of SaaS, PaaS, IaaS and on-premise IT solution management is explained using Figure 1 below.

Figure 1



3.0 IT Server & End-User Device Platforms

3.1 Because of the diversity of BCP Council's operations, it currently runs a complex mixture of commercial off the shelf systems, bespoke third-party applications and in-house designed, built and maintained systems, predominately running on Windows Server, with some instances of Red Hat Linux.

3.2 On-premise or Azure IaaS compatible IT solutions should detail server-side requirements and specifications clearly within proposals.

3.3 On-premise or Azure IaaS compatible IT solutions should detail all licensing requirements and restrictions, for example any limits on the ability to run multiple instances or perform disk or tape-based backups.

3.4 Where on-premise or Azure IaaS compatible IT solutions are implemented using platforms due to go end of life within the contract period (such as supported operating systems), suppliers must fully detail the migration effort and costs associated with keeping the solution in support.

3.5 BCP Councils end-user device estate is Windows 10 and all client-side requirements must be compatible with this operating system.

3.6 Windows 10 devices are currently being managed through Microsoft System Centre Configuration Manager (SCCM) Current Branch with an aspiration to move to a self-service orientated Windows Auto Pilot solution by April 2021.

3.7 BCP Council operates an extensive fleet of Android based mobile phones for its users currently managed through the M365 and Microsoft Intune platforms.

3.8 BCP Council operates a small fleet of iOS and Android based tablets (of various models) to satisfy niche client requirements. These are also managed through M365 and Intune.

4.0 Virtualisation

4.1 BCP Council has been a customer of VMWare for many years and has extensive in-house expert capabilities on this platform. All new on-premise servers will be virtualised under this platform unless there is a compelling business case not to do so.

4.2 BCP Council is looking to take advantage of the Windows Virtual Desktop platform to virtualise the deployment of applications to “hard to reach” employees & partners without ready access to Council provided end-user devices.

5.0 Databases

5.1 As might be expected with an organisation like BCP Council, there are a variety of database systems currently in use.

5.2 The IT Technical Strategy is seeking to reduce this complexity but BCP Council also recognises that "one size does NOT fit all".

5.3 BCP Council has extensive in-house expert capabilities in Microsoft SQL and as such this is the preferred database platform for on-premise, IaaS or PaaS solutions. Applications should be designed to avoid vendor-specific functionality.

5.4 Processes and functions used in maintaining the performance and integrity of BCP Council managed databases should be provided.

5.5 BCP Council will have a preference to deploy MS SQL services via PaaS.

6.0 Data

6.1 In support of the Organisational Development Plan and Digital Strategy, a vision for the Council as a data-led organisation is set out below:

6.1.1 Data and insight capabilities are embedded throughout service delivery and enhance the capability of staff to drive earlier interventions, leading to better identification of risks, allocation of resources and ultimately improved outcomes for people.

6.1.2 There will be a holistic view of a service users through the lawful joining up of data, ensuring that each interaction is relevant, streamlined and effective.

6.1.3 Services will be designed and refined using customer feedback and outcomes data, marrying qualitative and quantitative sources of information to focus on citizen outcomes through a rounded, service-agnostic approach.

6.1.4 Services will be more proactive and less reactive, driven by increasingly confident modelling and prediction, joining disparate sources of information to produce a single view of performance and finance that can be used to plan services, project demand and activity, and manage cost.

6.1.5 Data will be leveraged to provide targeting and build evidence bases for community services, as well as to hold commissioned services to account for the outcomes to which they contribute.

6.1.6 A learning and innovation culture will value and respect data, primarily through its centre of excellence and by learning from the strong business partnering arrangements that already exist.

6.1.7 Technology will be integrated to support the provision of services as one collective organisation. Procurement will be guided by a strategic roadmap that will outline a cohesive approach to system-related decisions.

6.2 In order to support these statements, suppliers must provide a full description of how they meet the Data Extraction and API requirements outlined below.

6.3 Data Extraction

6.3.1 Wherever permitted according to the General Data Protection Regulation, and all relevant data protection legislation:

6.3.2 The Council will have the right to recover, share, reuse and publish: all data that is entered into the system; any data that is augmented through the use of the system (e.g. linked data); and any data generated through the operation of the system.

6.3.3 The system must enable full copies of all system data to be extracted at any time at no additional cost to the Council. This should be in a structured, standardised (preferably open) and machine-readable format.

6.3.4 The Supplier will surrender, delete or return the system data to the Council at any time at no cost, at the request of the Council.

6.4 Application Programming Interfaces

6.4.1 Wherever permitted according to the General Data Protection Regulation and all relevant data protection legislation:

6.4.2 The system must have web APIs that enable the Council to give other applications full ability to send data to, or request data from it.

6.4.3 Specific requirements for these APIs include:

6.4.3.1 All significant business functions should be available via API

6.4.3.2 APIs should enable live data to be queried in real-time

6.4.3.3 APIs should support “Time Based Extracts” (e.g. data changed after date “X”) for both full system extracts as well as for more specific web API calls.

6.4.3.4 Any data that can be submitted by a user operating the system should also be able to be entered via API.

6.4.3.5 A complete register of all APIs must be provided to the council. All Open APIs must be discoverable.

6.4.3.6 All APIs must come with comprehensive documentation.

6.4.3.7 Where API access is restricted, a test API must be available. Ideally, test environment(s) should be provided that let developers test the API without affecting production environments.

6.4.4 These features must be provided without additional charge or limitation that would prevent the Council from accessing, sharing and using the data through the API.

7.0 Security

7.1 Of prime importance for any new system, especially internet facing ones, is the concept and implementation of security within IT solutions.

7.2 As BCP Council already operates internal systems that use or process payment card information and as the future direction of digital service delivery is likely to extend this capability much further, it is important that all designs, technologies, infrastructure, processes, and systems are specified, developed, and implemented fulfilling the requirements of the PCI-DSS (Payment Card Industry Data Security Standard).

7.3 Furthermore, and where applicable, proposals should state levels of adherence to the following standards:

7.3.1 ISO27001:2013 - the specification for an information security management system within a supplier's organisation.

7.3.2 ISO27017:2015 – the specification of a set of information security controls that must be implemented relating to cloud services.

7.3.3 ISO27018:2014 - the code of practice that focuses on protection of personal data in the cloud.

7.3.4 ISO22301:2012 - a best practice framework for implementing a business continuity management system, enabling suppliers to minimise business disruption in the event of an incident.

7.3.5 ISO9001:2015 – the specification for an ongoing quality management system within an organization.

7.4 All data must be securely stored in locations within the UK and in line with the Data Protection Act 2018.

8.0 Authentication and Authorisation

8.1 Third-party applications requiring local user access must integrate securely with Azure Active Directory (AAD) or, if appropriate, with the Councils on-premise Active Directory (AD) via native Kerberos or LDAP methods.

8.2 BCP Council uses on-premise AD internally to administer user and access control. Currently the Council is in the stages of migrating from its 3 legacy on-premise directories to a consolidated BCP Council AD and AAD.

8.3 Where a system is integrated with on-premise AD and external user application access is required then federated access must be utilised.

8.4 Please note that BCP Council will not extend its on-premise AD out to the internet or DMZ therefore AAD must be used in these instances.

8.5 Azure Multi-Factor Authentication is fully deployed to further control access from untrusted networks.

9.0 Remote Access

9.1 BCP Council provides remote access to on-premise, IaaS and PaaS applications and data to its staff via Microsoft DirectAccess and the Office365 web portal. In the future we will be transitioning to Microsoft Always On VPN. New systems and applications should be compatible with this approach.

9.2 BCP Council provides remote access to on-premise and IaaS applications to its IT support providers and partners by the following methods:

9.2.1 SSL VPN – BCP Councils secure web gateway and enabling RDP or SSH type connections to on-premise servers.

9.2.2 IPv4 VPN - IPv4 access from and to fixed IP addresses and ports on equipment in the Council's DMZ.

9.2.3 IPSec VPN – IPv4 access from unmanaged computers using Checkpoint client software to establish a VPN tunnel to the equipment in the Council's DMZ.

9.3 No other methods of remote access are supported or authorised.

9.4 Two factor authentication will be utilised for support providers and partners where appropriate.

10.0 Networks & Communications

10.1 BCP Council is currently implementing a new Multiprotocol Label Switching (MPLS) Wide Area Network (WAN) to underpin the provision of digital services.

10.2 This migration is set to complete by the end of 2020.

10.3 The MPLS has a 1Gb Internet connection on a 10Gb bearer.

10.4 The MPLS has a 1Gb Microsoft ExpressRoute connection on a 2Gb bearer.

10.5 BCP Council WAN sites will be served through a variety of 100Mb & 200Mb Fibre, EFM, EoFTTC and some legacy ECX connections to small sites.

10.6 BCP Council is migrating off its legacy on-premise VoIP telephony services to a modern Microsoft Teams SaaS based telephony solution with a single compatible SaaS Customer Contact Centre software solution.

10.7 This migration is set to complete by the end of 2020.

10.8 BCP Council will expect IT partners to be able to detail the bandwidth and network utilisation requirements of solutions.

11.0 Green IT

11.1 BCP Council has pledged to make its operations carbon neutral by 2030, and to work with the wider community to look at how early the Bournemouth, Christchurch and Poole region can be made carbon neutral, ahead of the UK target of 2050.

11.2 All new IT solutions are required to contribute to BCP Councils metrics on carbon consumption.

11.3 Proposals should state if they comply with any applicable recognised green standards, such as ISO14001.

12.0 Documentation

12.1 As with any system consistent and useful documentation is vital.

12.2 BCP Council will expect full and detailed system and service management documentation proportionate to the hosting arrangements in place.

13.0 Service Management Expectations

13.1 BCP Council will expect IT partners to state levels of adherence to the ISO 20000 standard and the service relationship and processes with the Council.

13.3 Due to the varied nature of BCP Councils operations, detailed Service Management expectations will be documented within specific IT solution procurements.

APPENDIX A: Borough of Poole Legacy IT Infrastructure

The current major elements of the IT infrastructure and standards that serve the Borough of Poole are summarised in the following table.

Cloud Asset	**Asset Description/Specification**	**Further Description**
Cloud Storage	Azure Cloud Storage	400Tb. West Europe - Amsterdam Datacentre
Servers	Azure Virtual Machine (IaaS)	MS-Server 2012 preferred. See Azure website for a full list of options.
Databases	Azure Database (PaaS)	MS-SQL 2012 preferred. Oracle is licensable in Azure.
Backup & Recovery	Azure VM Cloud Backup	North Europe – Dublin Datacentre / 30 day retention.
Connectivity	VPN	Upgrade to ExpressRoute as described above

On-premise Asset	**Asset Description/Specification**	**Further Description**
Storage Area Network (SAN)	Nimble CS1000	2 controllers – 8gb/s Fibre Hybrid SAS / SATA disk array
	Brocade SAN Switches	2 * 24 Port Fibre Channel Brocade 5100 Switches 1 * 8 Port Fibre Channel Brocade 3200 Switch
Backup & Recovery	HP MSL2024 Tape Device	
	Symantec 5240 Appliance	Disk-2-Disk-2-Tape Backup Strategy
	Backup Client Symantec Netback V 8.1.1	Includes agents for SQL, Oracle, Solaris and VMware.
Server Hardware	HP DL380 Racked Servers	
	HP Blade Infrastructure	3 Chassis (2 x Citrix + 1 x VMware)
	VMware Vsphere 6.5	
Server O/S	MS Server 2016 (32bit & 64bit) Windows Server 2008 R2 Domain	
	RedHat Linux 6.0	RedHat is our preferred/supported Linux flavour.
Thin Client	Citrix XenApp 6.5 OS – Windows Server 2008 R2 (64 bit)	Application Mode: Vendor Software must be capable of being packaged either by vendor provided packaging through command line install switches, or by the creation of an install package through 3rd party products, e.g. MSI repackage software

Email	Office 365	
	Office 365 Message Security	
Intranet (Loop)	SharePoint Online	
Internet (Bop.com)	Easysite CMS V7.6	
	Firmstep	
Database	Microsoft SQL2012 R2	Fully licensed corporate SQL cluster. Separate test/reporting infrastructure
	Oracle 11g release 2 or higher	
	Other RDBMS's	Alternatives to Microsoft SQL and Oracle will be considered where the application is of sufficient size to justify training and skilling overhead.
Office & Utility Software	Office 2016 & O365	
	Adobe Reader (PDF reader) Java Runtime Environment 8 Flash (current) Shockwave (current) VLC (DVD Player) 7Zip	All maintained at current version
	Sharepoint Foundation Server 2010	Functionality: Document Library, Workflow & Calendar.
	Adobe Creative Cloud Suite	Standard Publishing software
	SQL reporting / BIquery / Crystal reports	Standard Reporting tools
	Internet Explorer 11 / Chrome (Auto-update)	Internet presented content must support all industry standard browsers
	Dolphin Supernova Screen Reader	Accessibility Tool.
Network	Extreme Core / Edge LAN	Core Switches : Extreme VSP 8404 Core Switches Edge Switches : Extreme ERS 4900 series and Extreme XOS 440 Series Switches Server Switches : Extreme ERS 4900 Series and Extreme VSP 7200 Series Switches Network Management and Security : Extreme Management Centre and NAC. Topology : The two Extreme VSP switches are deployed in the network core and are interconnected using two 10GbE connections, forming a 20Gbps Link Aggr egation Group (LAG) or trunk providing a high capacity, resilient interconnect. The two core switches function as a resilient network core for server and edge switch connectivity. The edge switches and switch stacks are dual homed using 2 x 1Gbps connections to each core switch. Server switches are dual homed using 2 x 10Gbps to each core switch. The network is configured to use Extreme Fabric Technology.

	Dorset PSN (DPSN) WAN	Migrating to MPLS as described above
	PSN Gateway	Migrating to MPLS as described above
	HSCN Gateway	Dedicated link.
	Aruba Wireless LAN	Separated internet pipe for Public access.
Mobile	Devices: Various Handsets, Smartphones and Tablets	IPad is preferred Tablet device / Android Phone is preferred Smartphone. COPE (Corporately Owner Privately Provisioned) and BYOD both supported.
	Mobile Device Management – Microsoft Intune	
	iOS, Android, Windows8/10	
Corporate Telephony	Alcatel IPT Rel 10	Migrating to MS Teams as described above
	Updata SIP trunk	Migrating to MS Teams as described above
Security & Remote Access	Microsoft Forefront UAG 2010 SP3	
	RSA Authentication Manager 8.0	
	RSA Fob / RSA Software Tokens	
	Firewall Checkpoint Appliance R77,UTM1 & IP390	
	Microsoft Self Service Password Reset	
	McAfee EPO Server 4.6	Migrating to Trend and Defender
	McAfee VirusScan Desktop 8.7ip4 – Moving to Windows Defender	Migrating to Trend and Defender
	Device Encryption - Bitlocker	
	Web Filtering Websense WSv7.8	Migrating to Forcepoint Managed Service
	Splunk v6	
	TMG 2010 SP2	
	AD Manager Pro	
	Print Queuing - Funasset SPOOlQ V1.1g	
Operations & Secure Printing	Bac Bureau - C-series Bureau (Paybase v10)	
	Canon uniFLOW 5.4	Managed Print Service

Print Management	Lagan 8.0.5	Replacement with CEM system agreed
CRM	SCCM 2007 R2 – Moving to SCCM Current Branch	
Desktop Management	License Manager V5.8	connected to SCCM and Dashboard Discovery
License Management	Sostenuto 5.4	
Service Desk	Idocumentsystems (IDOXS) 5.0	
Document Management	Windows 7 – Moving to Windows 10	
Desktop O/S	Dell Laptops	
Desktop Hardware		

APPENDIX B: Bournemouth Borough Council Legacy IT Infrastructure

The current major elements of the IT infrastructure and standards that serve legacy Bournemouth Council are summarised in the following table:

Cloud Asset	**Asset Description/Specification**	**Further Description**
Storage	Storsimple Appliance (On-premise)	Series 8100
	Azure Cloud Storage	400Tb. North Europe - Dublin Datacentre
Servers	Azure Virtual Machine (IaaS)	See Azure website for a full list of options.
Databases	Azure Database (PaaS)	MS-SQL 2012 preferred. Oracle is licensable in Azure.
Backup & Recovery	Azure VM Cloud Backup	West Europe – Amsterdam Datacentre / 30 day retention.
	Storsimple Cloud Clone	Can be created in cloud from backups during a DR scenario.
	Storsimple Backup	Full + changes
Connectivity	VPN	Upgrade to ExpressRoute as described above

On-premise Asset	**Asset Description/Specification**	**Further Description**
Storage Area Network (SAN)	EMC VNX 5600	
	Brocade SAN Switches	2 * 24 Port Fibre Channel Brocade 5300 Switches
Backup & Recovery	Scalar LTO 4	
	Data Domain	Disk-2-Disk-2-Tape Backup Strategy
	Networker 18.1	Includes agents for SQL, Oracle, Solaris and VMware, HyperV
Server Hardware	HP DL380 Racked Servers	
	VMware Vsphere 5.5 HyperV Window Server 2012	
Cloud Platform	Microsoft Azure	
Server O/S	MS Server 2012 (32bit & 64bit) Windows Server 2008 R2 Domain	2008R2 being removed from service. All new services will be MS Server 2012 minimum
	RedHat Linux 6.0	RedHat is our preferred/supported Linux flavour.

Thin Client	Citrix XenApp 6.5 OS – Windows Server 2008 R2 (64 bit)	Application Mode: Vendor Software must be capable of being packaged either by vendor provided packaging through command line install switches, or by the creation of an install package through 3rd party products, e.g. MSI repackage software
Email	Exchange O365	
Intranet BCP	SharePoint Online	
Internet	https://www.bcpcouncil.gov.uk	
Database	Microsoft SQL2012 R2	Fully licensed corporate SQL cluster. Separate test/reporting infrastructure
	Oracle 11g release 2 or higher	
	Other RDBMS's	Alternatives to Microsoft SQL and Oracle will be considered where the application is of a sufficient size to justify training and skilling overhead.
Office & Utility Software	Office 2016 and O365	
	Adobe Reader (PDF reader) Adobe Air (W10) Java Runtime Environment 7 Flash (current) Shockwave (current) DWG Trueview 2013 Media Player 11 Quick Time 7 Silverlight 5 VLC Media Player 7 Zip	maintained at current version
	Sharepoint Microsoft O365	
	Adobe Creative Suite CS5/6	Standard Publishing software
	SQL reporting / BIquery / Crystal reports	Standard Reporting tools
	Internet Explorer 11 / Chrome / Edge	Internet presented content must support all industry standard browsers. Updates centrally controlled
	Dragon Naturally Speaking	Accessibility Tool.
Network	Extreme Core / Edge LAN	Core Switches : Extreme VSP 8404 Core Switches Edge Switches : Extreme ERS 4900 series and Extreme XOS 440 Series Switches Server Switches : Extreme ERS 4900 Series and Extreme VSP 7200 Series Switches Network Management and Security : Extreme Management Centre and NAC.

		Topology : The two Extreme VSP switches are deployed in the network core and are interconnected using two 10GbE connections, forming a 20Gbps Link Aggregation Group (LAG) or trunk providing a high capacity, resilient interconnect. The two core switches function as a resilient network core for server and edge switch connectivity. The edge switches and switch stacks are dual homed using 2 x 1Gbps connections to each core switch. Server switches are dual homed using 2 x 10Gbps to each core switch. The network is configured to use Extreme Fabric Technology.
	Aruba Wireless LAN	Separated internet pipe for Public access.
Mobile	Devices: Various Handsets, Smartphones and Tablets	Ideally Windows Tablet. Alternatively, iPad device / Samsung Android Phone is preferred Smartphone.
	Mobile Device Management – Intune	Hybrid – SCCM Current Branch
	iOS, Android, Windows8/10	
Corporate Telephony	Nortel CSK1000	
	ISDN 30	

Security & Remote Access	Firewall Infrastructure External Perimeter Security = PaloAlto Cluster DMZ Load Balancing = F5 Internal Firewall and DMZ = Checkpoint 4400 in a cluster	
	Trend Micro 11.6	Anti Virus
	Microsoft Self Service Password Reset	
	Forcepoint Web Security Cloud 2019	Web Filtering
	Clearswift Secure E-mail Gateway Exchange O365 EOP & OME	Mail Encryption Clearswift being replaced with O365 included products
	Symantec Messaging Gateway	Mail filtering

	Juno Pulse 5.1	Remote VPN software
	MS Direct Access (W10)	Remote Wifi / VPN Software
Operations & Secure Printing	Print Queuing - Cheque Write - CheqXpress	
Print Management	Canon uniFLOW 5.0.5	Managed Print Service
CRM	MS Dynamics	
Desktop Management	SCCM 2007 R2	Upgrade to SCCM 2016 in progress
License Management	License Manager V5.8	connected to SCCM and Dashboard Discovery
Service Desk	Sostenuto 5.4	
Document Management	Wisdom eDRM 8.0	
Desktop O/S	Windows 7 SP1	Windows 10 rollout in progress

Desktop Hardware	Desktop: HP EliteDesk 8200, 8300, 800	Standardising on Dell laptops
	Desktop: Dell 5060 MicroPC	Standardising on Dell laptops
	Laptop: HP ProBook 6560,6570 & 650. Elitebook 2570p & 820	Standardising on Dell laptops
	Laptop: Dell 7390, 7490, 7390 2 in 1, 5290 2 in 1	Standardising on Dell laptops

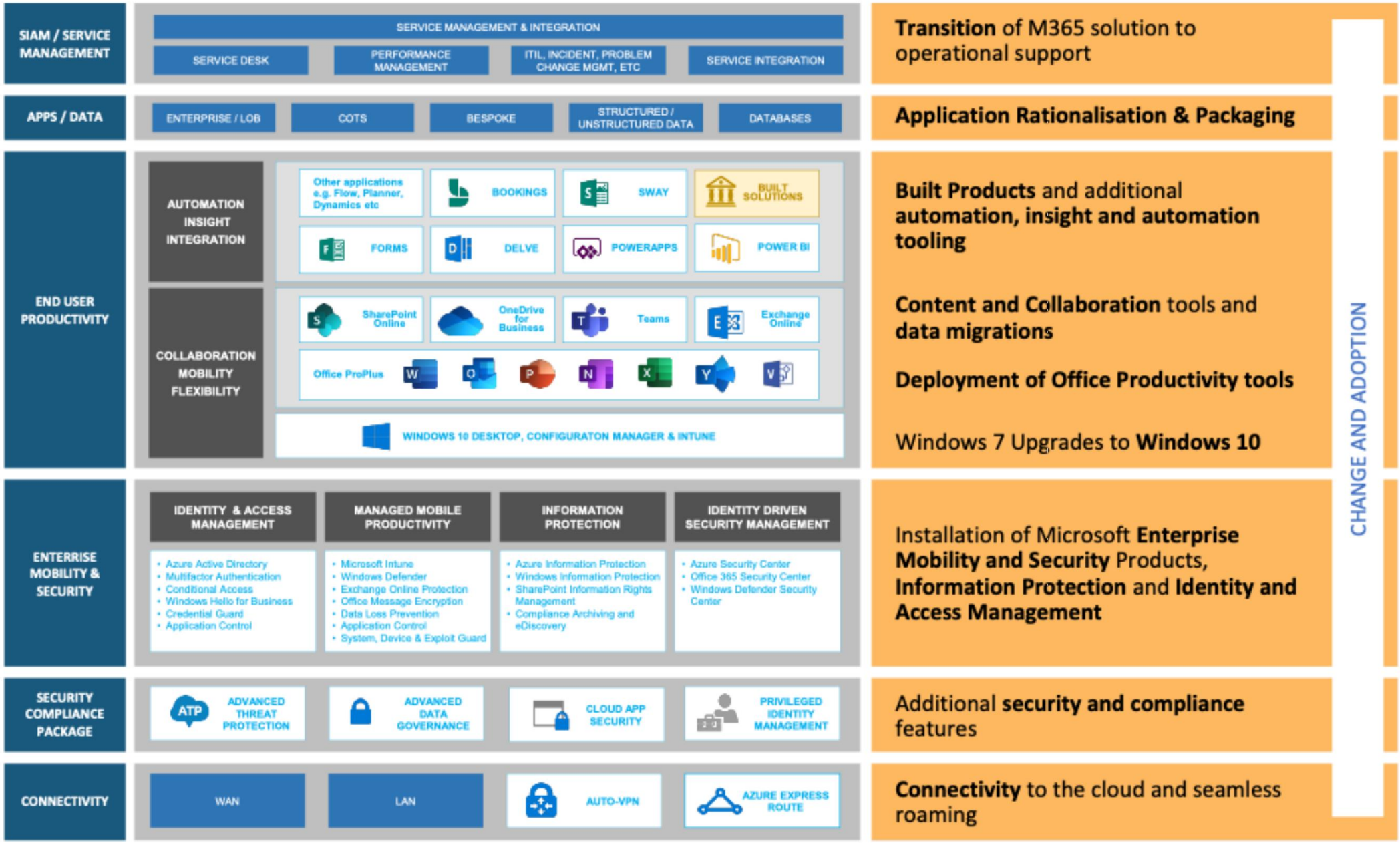
APPENDIX C: Christchurch Borough Council Legacy IT Infrastructure

The current major elements of the IT infrastructure and standards that serve Christchurch Borough Council are summarised in the following table:

On-premise Asset	**Asset Description/Specification**	**Further Description**
Storage Area Network (SAN)	Nimble CS3000 Hybrid Adaptive Flash Array	33 TB Usable Capacity
Backup & Recovery	HP MSL2024 Tape Autoloader	LTO7
	Veeam Backup and Replication	Enterprise Plus 9.5
Server Hardware	HP DL360 G9 Racked Servers	
	VMware Vsphere 6.0	
Server O/S	Windows Server 2008R2 Windows Server 2012 Windows Server 2012R2 Windows Server 2016	2008R2 being removed from service. All new services will be MS Server 2012R2 minimum
Thin Client	RDS Server 2012R2	
Email	Exchange O365	
Intranet BCP	SharePoint Online	
Internet	https://www.bcpcouncil.gov.uk	
Database	Microsoft SQL2012 and above	
Office & Utility Software	Office 2016 and O365	
	Adobe Reader (PDF reader) Java Runtime Environment Flash (current) Silverlight 5	maintained at current version
	Sharepoint Server	
	Adobe Creative Suite	
	SQL reporting server	

	Internet Explorer 11 / Chrome / Edge	Internet presented content must support all industry standard browsers. Updates centrally controlled
Network	HPE/Aruba LAN Switches	Core: HPE/Aruba 5406R Chassis (10GbE & 1Gb) Edge: HPE 2920-48G-POE+ Transit: HPE 2910al 24G
	Aerohive AP320 Access Points	Corporate, guest, and public wifi access Public internet access via isolated BT Infinity filtered broadband
Mobile	Devices: Various Android Handsets, Smartphones	Samsung Android Phone is preferred Smartphone.
	Mobile Device Management – Intune	
Corporate Telephony	Microsoft Skype for Business on-premise Enterprise Voice	
	SIP Trunk	50 channels (6Mbps PureIP MPLS) AudioCodes Mediant 800 Active/Passive SBCs

Security & Remote Access	Firewall FortiGate 101E (internal facing stack and external facing stack) FortiNet FortiAnalyzer 200D	
	Microsoft Endpoint Protection	Anti-virus
	Forcepoint (Websense) Triton AP-Web Cloud service	Web Filtering
	Exchange O365 EOP & OME	Mail filtering and encryption
	Juno Pulse 5.1	Remote VPN software
	Microsoft Bitlocker	Device Encryption

	Microsoft Direct Access	Primary remote access technology for corporate users
	Northbridge NetConnect SSL VPN	Secondary remote access technology SSL VPN for non-corporate user access - Vasco 2FA (hardware and software tokens)
	Splunk	SIEM
	Specops Password Policy	
Print Management	Konica	Follow-me Printer services
Desktop Management	Microsoft Configuration Manager Current Branch	
Service Desk	Sostenuto	
Desktop O/S	Windows 10	
Desktop Hardware	Dell 5300 2-in-1	

APPENDIX D: M365 within BCP Council