1. Technical Strategy

1.1 Introduction

Although this document will at a later date form part of the wider ICT strategy, it is intended as a standalone technical document to be used to provide direction and product selection guidance to ICT technical staff and management at ECDC.

It is vital that the Council keeps its options open to enable it to react to a rapidly changing ICT market place and to exploit opportunities that may come its way. The components of the technical strategy, as set out below, will deliver a flexible platform, which:

- Can be supported by staff with a wide mix of skills
- Means that the council does not lock itself into any technology or supplier which then precludes it from exploiting these wider opportunities

It is the intention to revisit the technical roadmap on an annual basis as longer term elements are difficult to predict and it is important to adjust the overall strategy 'in flight' to take advantage of opportunities within new technical developments.

It should also be noted that over the past few years there has been a significant investment in distributed infrastructure (a desktop refresh mostly involving the replacement of fixed PCs) but the core infrastructure has become end of life, at capacity and is becoming difficult to support. In particular, storage, virtualisation, resilience, service recovery, data security, data networks and telephony are all at the point in the cycle where further investment and refresh is required.

There are other wider initiatives and developments that have driven the general concepts of the technical strategy, including an emphasis for on-premise solutions, these are:

- The remote and rural location of ECDC offices and lack of connectivity to other council owned locations.
- Participation in the Cambridgeshire PSN network.
- A general lack of resilience and investment in recovery processes.
- Emphasis on minimising future Revenue spend, driving the capital model (spend to save, sweat the asset) rather than the rental model.

Within the technical strategy we have discussed the themes of the short (2016), medium (2017) and long (2018 and beyond) term. Obviously any certainty around actual strategy developments beyond 2018 is difficult to predict and are general themes rather than specifics. As such, the technical strategy is intended to be a rolling strategy that is reviewed on an annual basis and adjustments made accordingly.

High Level Key Themes

- Investment in core infrastructure to improve customer efficiencies, reliability (through greater resilience in the design), consolidation and to provide modern functionality.
- Support the wider transformation programme by providing true 24x7 services and meeting the needs of the digital by default strategy.
- Drive out year on year savings (revenue costs) by investing in on-prem solutions that have low on-going support requirements.
- Adopt a Microsoft strategy, as ECDC is committed to an Enterprise Subscription agreement, whereby Microsoft software is used by default unless there is no product available.
- Offer an effective Disaster Recovery solution that can be adapted to a further BCP.

- Deploy effective solutions to enable mobile and agile working over the period of this strategy.

1.2 Core Infrastructure

As with most organisations, the ICT core infrastructure has become highly developed and complex in design, requiring the in-house team to forge partnerships with a number of specialist suppliers for design, configuration, support and project delivery services.

Key Themes that are likely to emerge over the coming years that will impact on the ICT technical strategy are:

- Smaller footprint across the whole core infrastructure piece is driving lower cost core computing in smaller server rooms.
- Performance improvements through increasingly faster processors, Solid State Disks (SSD) and increasing memory capacity.
- Selling capacity – the ability to use storage/compute and network capacity in-house and across the internet is driving opportunities for alternative ways of delivering line of business applications.
- Cloud service delivery including Software as a Service (SaaS) and on-line storage may provide the opportunity for cheaper service delivery through the removal of on-premise data centres.
- The continuing growth of data storage and retention, and the number of servers required to deliver the range of ICT services demanded.

In brief, this technical strategy is cautious over the use of cloud and is predominantly an on-premise service delivery strategy only choosing cloud services where individual business cases are strongly in favour of cloud delivery. However, as with other emerging technologies, a regular (annual) review of this position is recommended.

1.2.1 Data Centres (Server Rooms)

Server rooms at the Grange have evolved during the period of the last strategy into two separate units on the ground and first floor. This over complication of design was initial due to space requirements but with the footprint of modern equipment and the aim of full virtualisation the strategy of dual server rooms is no longer necessary.

Whilst the aim is to consolidate at the Grange there is also a need to identify a location and build a secondary server facility for Disaster Recovery purposes.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Data Centres (Server Rooms)	• Create a robust on-premise infrastructure • Consolidate into a single ground floor facility • Decommission first floor facility • Reduce running costs of the primary data centre	• Introduce a secondary data centre • Identify and remove single points of failure • Reduce footprint	• Review on-prem strategy and exploit cloud services for PaaS where relevant

	• Identify location for secondary data centre		

1.2.2 Storage

The current core storage is at capacity and is based on end of life hardware. There is a 2016 project identified to provide replacement hardware that will offer ECDC sufficient capacity for the next 5 years and the performance required to delivery effective core and line of business applications. Storage will be presented at both a primary and secondary site offering both resilience and recovery options.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Storage	• Replace ageing storage with new robust solution • New storage to support scalable disaster recovery • Reduce footprint • Increase performance and resilience	• Deliver an effective recovery solution • Introduce storage tiering • Introduce data and email archiving	• Review on-prem strategy and exploit cloud services for PaaS where relevant

1.2.3 Servers & Appliances

ECDC is similar to most other Local Authorities who run Microsoft operating systems, in that there are currently three server versions currently on the network. However, with a strategy in-place to decommission the remain Server 2003 servers by late-2016 and to move to 2012 over the lifetime of this strategy, good progress towards a single server version is being made.

Physical appliances are still common place in the environment although, where security standards allow, the introduction of virtual appliances is the preferred standard.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Servers	• Through the storage refresh project, reduce primary server nodes from 6 to 4 • Decommission all Server 2003 servers • Standardise on Server 2012 using data centre licencing for core platform	• Exploit all the advantages of Server 2012 server and domain functionality	• Server 2008 end of life Jan-20 – plan replacement of all 2008 servers • Review cloud options and move compute power to PaaS where a business case exists • Replace Dell compute nodes as required

1.2.4 Virtualisation

Both virtualisation software and the percentage of virtualised servers needs addressing in the short term. VMware is two versions behind and is at end of life and the numbers of servers that are still physical is around 30%.

The 2016 infrastructure refresh offers new possibilities for virtualisation along with an opportunity to exploit Microsoft virtualisation software (Hyper-V) provided as part of the Enterprise Subscription Agreement.

Although VMware is still considered as the market leader for server virtualisation it is not the cheapest and there are now more viable alternatives. The case for considering Microsoft's Hyper-V is increasing, particularly when an organisation is committed to Microsoft enterprise licencing for a long period of time where significant costs savings can be realised.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Virtualisation	• As part of the storage project, migrate server to Hyper-V • Target 80% virtualised servers • Virtualise DMZ servers	• Complete migration to Hyper-V • Realise savings in VMware licencing • Target 90% virtualised servers	• Review suitability of infrastructure virtualisation and consider market trends in desktop virtualisation

1.2.5 Authentication

Microsoft Active directory within a single domain model is used for primary desktop authentication. There are no plans to evaluate alternatives to Microsoft authentication and it is likely to remain relevant, even beyond any commitment to cloud infrastructure, as it offers local directory services.

The deployed version, Server 2008, becomes unsupportable in 2020 and therefore the short to medium term plan is to implement Server 2012 and upgrade the domain version accordingly.

The use of Active Directory Federated Services (ADFS) for the authentication of external services such as cloud based line of business applications is a likely extension of active directory that will need to be considered in the medium term.

Single sign-on remains a challenge with some line of business applications maintaining their own user identity services. This is common to most Local Authorities despite the strategy maintaining that AD should be used for all authentication purposes.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Active Directory Authentication and design	• AD 2008 native is currently strategic • Single sign on authentication deployed where possible • Policy is to buy only	• Upgrade AD to 2012 version • Introduce ADFS for single sign-on for cloud based applications such as O365 and hosted line	• Continue to aim for single sign-on across all council applications

	AD integrated software • AD schema update to support SfB 2015	of business applications	

1.2.6 Disaster Recovery

ICT is developing an advanced Disaster Recovery design during 2016 using products from Microsoft, ArcServe and Dell, capitalising on server virtualisation and data replication technologies. This is in contrast to the lack of a recovery mechanism and plan that has existed at ECDC for some time.

The solution will provide rapid recovery capability for systems deemed by ICT as critical with a detailed approach for building out the recovery environment for second tier services should a disaster be extended. The provision of 'bums on seats' capability at a nominated ECDC remote site will also form part of the plan. It should also be recognised though that the business does not have a clearly defined BCP and recovery priorities / SLA should be being driven by the business and not ICT.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Disaster Recovery	• Identify DR location (standby site) • Provide DR connectivity • Integrate the strategic ArcServe UDP product with the new replicated storage deployment • Utilise ArcServe UDP to recover data to primary / secondary locations • Produce a strategic DR plan	• Work with Asset Management Team to support the emerging BCP • Complete the installation of the DR infrastructure • Basic DR tests in conjunction with BCP scenarios	• Fully test DR Capability • Look to introduce VM fail-over between data centres

1.2.7 Core Networking

Core switching is currently based on HP ProCurve hardware and provides a 10Gbps core on a chassis based switch with fibre links to edge switching. Some components of the core network are approaching end of life and will be addressed during 2016.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Core LAN	• Review Core switch requirements and plan around component end of life	• Consider further resilience and test device failure scenarios	• Review device life-cycles

	• Consider the topology of the network (core-edge or mesh) • HP hardware to remain strategic • iSCSI (Ethernet) to remain strategic for data core • Separate SAN traffic from LAN traffic • Obtain adequate hardware support for core LAN hardware		

1.2.8 Wide Area Network (WAN) / Internet Connectivity

ECDC is committed to the Cambridgeshire Public Service Network (CPSN) which offers inter-site, internet, guest wifi services and PSN connectivity. The MPLS core network is managed by CPSN providing 'tail' circuit connectivity to public organisations within the Cambridgeshire area.

ECDC has a non-resilient connection at Ely which is segmented to provide the services previously mentioned.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
WAN / Internet	• Continue the strategic relationship with CPSN • Provide DR site connectivity through an additional tail circuit • Move WAN circuit to ground floor server room	• Strategic review as CPSN framework agreement ceases in 2018 • Review of long-term bandwidth requirements and resilience needed to support cloud services •	• Further WAN connectivity subject to 2017 review and market pricing for alternative services

1.3 Distributed Infrastructure

1.3.1 Desktop Devices

The focus during 2016 will be on the completion of the device roll-out and the re-cycling of old devices. The current round of updated, that commenced in 2014, is another refresh of the exiting fixed PC approach with Windows 7 and Office 2007 forming the base build.

In the medium term, a review in readiness for the next desktop refresh will be required both from a hardware (device) and software (operating system and office software) perspective. Although this strategy maintains that cloud is not the default approach, ahead of the next desktop build it would

be prudent to assess the success or otherwise of the use of Office 365 and Azure storage by the trading company.

The main desktop offering will be supplemented with other more mobile solutions (Laptops and Tablets) where necessary. However, it will be a requirement of the business to determine when and in what circumstances mobile devices are applicable.

Element	Short-term (2016/17)	Medium-term (2017/18)	Long-term (2018 and beyond)
Desktop Devices	• Continue with 'thick' PC desktop devices in the short-term, supplemented by laptops where applicable • HP to remain the strategic supplier of desktop devices • Gold image development and deployment tool via strategic Microsoft MDT software • Windows 7 with Office 2007, moving where possible to Office 2013 is the strategic desktop deployment • Review of monitors required • Desktop review to establish the long term strategic requirement	• Office 2007 end of life (October 2017) • Tactical monitor upgrade • Tactical laptop deployments • New desktop builds via golden image and deployment tool	• Desktop refresh • Windows 7 end of life Jan-2020 • Strategic build to be Windows 10 • Office 2010 end of life date is 10/2020 • Full adoption of O365 by 2020 is an option

1.3.2 Edge Switching

As with the core, ICT deliver a robust desktop connection using HP ProCurve switching. With 10Gbps interconnects and 1Gbps delivered to every desktop, performance across the LAN is easily capable of providing the capacity for all current and future systems.

Work to provide PoE switching and a review and upgrade of switch hardware components approaching end of life will be undertaken in the short-term.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Edge Switching	• HP ProCurve remains strategic • PoE throughout to support VoIP	• Roadmap review for specific hardware deployed • Review resilience	• Plan to replace any hardware that approaching end of life

	• 1Gbps direct to each desktop to be shared between data and voice • Review support contracts for key components	within the design	

1.3.3 Wireless Networks

Wireless connectivity is restricted to a public / guest (BYOD) facility provided over the CPSN WAN. Coverage is reasonable and performance adequate for casual Internet access.

Many local authorities are now providing corporate wireless access to enable employees to access systems and files when away from their desks, but given the mainly fixed nature of the ECDC desktop this may not be seen as very relevant in the short-term.

There is no suggestion that, within the lifetime of this strategy, wireless will replaced wired in the Grange offices as the primary connectivity method but advances in wireless technologies such as 802.11ac and controllerless environments should be closely monitored.

An ever increasingly mobile workforce will demand wireless connectivity on the move. Although ICT cannot control access in the public domain it will need to be aware of trends and availability to offer connectivity for all mobile devices and proved advice to customers on how to stay connected.

Element	Short-term (2016/17)	Medium-term (2017/18)	Long-term (2018 and beyond)
Wireless	• CPSN public / guest wifi to remain strategic for ad-hoc Internet connectivity • This solution is fit for purpose but does not exploit wireless capability to the full • Aruba Access Points remain strategic	• Introduce corporate wifi over existing access points for mobile users • Review strategic requirements of services delivered via CPSN in preparation for framework agreement ending in 2018	• Align wifi with new desktop / mobile solution

1.3.4 Remote & Flexible Working

The current AEP SSL VPN solution with Vasco 2-Factor Authentication (2FA) provides an adequate solution for casual home workers who provide their own equipment. It relies on additional software being installed on the client device and is of a non-resilient design.

It will be important to align the home working solution with the desktop device strategy as with the anticipated move towards mobile devices and potential for pattern based home working there will be a need to improve both the resilience and the performance of remote access.

Future trends may require 'always on' services based on certificated authentication with data and systems being stored in multiple locations. Member access, BYOD and the use of devices as small as

smartphones through to large screen 'docked' laptops will certainly stretch the capability of such solutions.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Remote Working	• Strategic solution is SSL VPN currently via AEP and over RDS desktop • Review of options – consider Microsoft Direct Access • Vasco 2FA tokens remain strategic • Limited OWA access remains • Tactical upgrade to SSL VPN to improve resilience and performance	• Review the use of managed and unmanaged devices • SSL VPN with 2FA for unmanaged devices • Always on SSL VPN with certification introduced for managed devices • BYOD for staff limited to smartphone access •	• Use of O365 will affect the delivery model • More mobile workers aligned to an enhanced home working policy will drive future remote access solutions

1.3.5 Printing Services

Most Borough/Districts now have a leasing agreements in-place for MFD printing leaving ICT only to deal with the print server function and reporting. The move to 100% MFD printing requires management buy-in and often corporate / management team policy. ECDC needs a further drive towards removal of all standalone printers but this cannot be achieved by ICT alone.

Considerable savings in both ad-hoc consumables and support time can be made through the adoption of managed print services.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Printing services	• MFDs are strategic with Follow Me printing • Phase out local printers (requires management support) • Konica are the strategic hardware supplier	• 100% MFD – remove remaining standalone printers • Move to centralised Konica MFD management • Increase MFD availability where required	• Review contract

1.4 Telephony

1.4.1 Fixed

During 2016 ECDC will begin to see the move towards a modern Voice over IP solution by leveraging the investment already made in the existing (Customer Contact Centre only) Mitel telephony deployment.

The strategy will be to provide modern VoIP services to all council staff whilst removing the old analogue service which is end of life and expensive to support.

Once the initial VoIP deployment is complete, the council can then move to SIP for the delivery of external DDI ranges offering greater flexibility for service recovery and further reductions in call costs.

Instant Messaging (IM) as part of Unified Comms (UC) will be introduced after a trial of Mitel and Microsoft products.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Core and Fixed Telephony	• Mitel is the strategic VoIP solution • Expand the use of Mitel controllers and roll-out new handsets to all staff • Decommission old TDM telephony system • Implement IM for UC, initial trial in ICT including Presence Awareness • Plan for removal of analogue external services for DDIs	• Complete IM deployment • Move to SIP • Deploy teleworker • Ensure staff and trained and aware of new functions	• Review calls and lines contract

1.4.2 Mobile Telephony

- Corporate Devices

Despite the growth in Bring Your Own Device (BYOD), during the period of this strategy, there will continue to be a need for corporate handsets due in part to user preference but also to satisfy specific needs. The current contract with Vodafone is due to be reviewed during 2016 and opportunities may exist to introduce new suppliers and/or negotiate a handset refresh fund with pooled data as part of a new contract.

- BYOD

There is a short-term need to deploy an MDM (Mobile Device Management) solution to support user owned devices. This Sandboxed solution offers customers the choice of using their own handset but with access to Corporate data such as email, calendars and attachments. This type of solution often satisfies customers who would prefer not to have two handsets, members who supply their own equipment and often results in the removal of the outdated and insecure OWA (Outlook Web Access).

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Mobile	• Select an MDM	• Re-let the Vodafone	• Complete

	solution that meets the council's requirements – trial in ICT • Review the use of Blackberry devices • Standardise on handset models for corporate devices • Review the corporate mobile phone contract currently with Vodafone	corporate contract (or alternative) • Introduce BYOD via MDM as an alternative to corporate handsets • Introduce shared data pooling for cost savings • Refresh corporate handsets as part of a roll-out	corporate handset refresh • Align mobile phone solution to desktop strategy

1.5 Data & Systems Security

The PSN Code of Compliance (CoCo) continues to drive Local Government ICT and Data security requirements with the annual ITHC (Health Check), quarterly internal scanning and the submission of the annual report to the cabinet office. ICT continues to meet the requirements of the CoCo and has a thorough approach to meeting the standards.

There is a requirement to establish the role of Senior Information Risk Office (SIRO) as recommended within ISO27001; someone who is detached from the general day to day running of ICT at a technical design level.

There is a need to establish an active Information Governance Group (IGG) that provides the vehicle for policy review, introduction of new policies and the sign-off against risk.

ICT has deployed and supports a suite of security products that offer comprehensive protection across all platforms. The maintenance and continual upgrade of these products is critical to meeting the continued and growing threat to data security.

Element	Strategic Products	Considerations
Device Encryption	• Microsoft BitLocker	• Strategic product • Central management required • USB flash memory to be considered
Anti-Virus (Desktop & Servers)	• Kaspersky	• Strategic product • Consider Trend Micro in long-term
Two-factor Authentication	• Vasco currently in use	• Consider alternative 'soft' tokens via SMS/SMTP • Consider certificate based authentication for trusted devices
Mail filtering	• On-prem Symantec mail gateway with on-line quarantine	• Integrate with O365 as required • Consider Mailsafe in the long-term
Web Filtering	• Zscaller cloud solution	• Strategic product

		• Cloud integration required
Firewalling	• Forcepoint (Stonesoft)	• End of life 2016 • Consider Paloauto • UTM/IDS devices required • Separation of PSN • Resilient design required • DMZ to move from physical to virtual
Patching	• Current tactical approach is WSUS with ad-hoc use of PDQ	• Move to ManageEngine Desktop Central to supplement the use of WSUS (Microsoft & non-Microsoft patching)
Log Aggregation	• ManageEngine Event Log Analyser	• Strategic product
Vulnerability Scanning	• Nessus Professional	• Strategic product

1.6 Software Licencing

Microsoft software remains a major and strategic part of both Server and Desktop solutions. This wide adoption will continue throughout the period of this strategy with version updates required to remain compliant and a continued commitment to the Microsoft ESA (Enterprise Subscription Agreement).

The Microsoft licencing model can be confusing and expensive, but with a significant amount of licencing within the ESA some complications such as numbers of licences required due to growth are remove with the annual true-up arrangements. However, this type of licencing agreement is basically a rental model where at the end of the agreement the authority does not own the licences and is left with a decision; continue to rent or buy outright.

Enterprise agreements can also be affective where there is wide adoption of Microsoft products (if Microsoft provide the functionality then it should be deployed) and where the organisation has a strategy to deploy the latest versions of products. As such, given the commitment to an ESA, these two points should be fundamental to the strategy.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Microsoft Software Licencing	• ESA is strategic with a current term of 3 years • Utilise Software Assurance where programme allows • Deploy Microsoft solutions by default	• Continue to exploit ways of achieving best value from the agreement	• Review ESA
Other infrastructure software	• Migrate away from Java • Continue to update Adobe • Manage Engine Opmanager for	•	•

	systems, server and network monitoring • Introduce Desktop Control for inventory		

1.7 Infrastructure & ICT Software Choices

Listed below is specific Infrastructure software (non-line of business) not covered in the sections above.

Element	Short-term (2016)	Medium-term (2017)	Long-term (2018 and beyond)
Exchange	• Exchange 2010 is strategic • Resilient solution through DAG but not site resilience	• Decision on 2016 version upgrade or move to O365	• Exchange 2010 end of life Jan-2020
Internet Browser	• IE11 is strategic and included in current Windows 7 build	• Review browser versions – align to desktop build	• Review browser versions – align to desktop build
Database strategy	• SQL is strategic • Standard version is 2008 – end of life July-2019 • Removal of single 2005 database is imminent – end of life April-2016	• Create an enterprise cluster • Plan to move to 2012 or 2014 following a version review	• Consider cloud hosting for database solutions
File storage	• Microsoft Server 2008	• Microsoft 2012 • Consider if limiting folder storage by department is desirable	•
Server Desk and change control	• SpiceWorks free version currently deployed • Alternatives are being considered	•	•
Inventory	• SpiceWorks free version currently deployed • Supplemented by free version of PDQ • Decide on Desktop Central or PDQ and procure full versions.	•	•

1.8 Strategic Partners

To provide effective support and specialist expertise for a continually more complex range of hardware and software solutions, the in-house team has a number of trusted partners. These range from formal agreements, usually 1 year, for a specific level of support and advice to less formal 'as and when' arrangements for ad-hoc services. The table below sets out our strategic partners against each area of the infrastructure.

Element	Product / Service	Strategic Partner
Desktop	RDS	
Desktop	HP Devices	
Email	Exchange	
Database administration	SQL	
Authentication	Active Directory	
Telephony	Mitel	
Telephony	Corporate Vodafone Mobile	
Telephony	BYOD / MDM	
Telephony	Handsets	
Computer Room	UPS	
Storage	Nexus/DotHill	
Servers	Dell	
Hypervisor	VMware	
LAN	HP	
Printing	Konica	
Remote Access	AEP / Vasco	
Backup & DR	ArcServe UDP	
Software Licencing	Microsoft	
Data Security	Annual Health Check & Scans	
Service Desk	SpiceWorks	
Disposal	WEEE compliant disposal	
WAN	CPSN / VMS	
Wireless	CPSN / Aruba	

Appendix A – Glossary of Terms

PSN	Public Sector Network	Access to secure government services and data exchange via a private government network. In ECDC's case, the Cambridgeshire PSN built on Virgin Media connectivity.
BCP	Business Continuity Plan	The wider plan covering major issues within the district that may also affect the council's ability to carry out its normal functions.
DR	Disaster Recovery	An ICT plan to recover systems and services following a major outage affecting core services.
On-prem	On Premises Service	Hardware and Software services that are hosted from ECDC buildings.
Cloud	Including Software as a Service (SaaS), Platform as a Service (PaaS), etc.	Hardware and Software services hosted in data centres outside of the council, either accessed via the Internet or over private network circuits.
Server Virtualisation	VMware Vsphere & Microsoft Hyper-V are types of hypervisor	Ability to run multiple server instances on a single physical server.
Hypervisor	VMware Vsphere & Microsoft Hyper-V are types of hypervisor	The software that allows a number of servers to share a single hardware platform. Shared processors, memory, network cards.
DMZ	Demilitarised Zone	A protected area of the network between the trusted LAN and the WAN/Internet.
SAN	Storage Area Network	Storage / Compute / Network infrastructures where line of business applications and hosted and data is stored.
LAN	Local Area Network	The network within ECDC building. Internal and private.
WAN	Wide Area Network	The partially private network connecting ECDC buildings and other Cambridgeshire public organisations.
PoE	Power over Ethernet	The ability to power telephony handsets and other small devices over the Ethernet network.
BYOD	Bring Your Own Device	The use of non-corporate devices to access council data secure MDM software.
2FA	2-Factor Authentication	Providing multiple authentication methods such as username, password and PIN to access corporate data remotely.
OWA	Outlook Web Access	A last generation method of accessing corporate email via a browser.
MFD	Multi-Function Devices	Large printing, scanning and copying devices with proximity card print release systems. These devices have pretty much replaced standalone printers in most businesses.
VoIP	Voice over Internet Protocol	A way of using the structure cabling system to connect and patch telephony handsets for digital telephony systems.
TDM	Time-division multiplexing	Legacy analogue telephony systems use this

		technology for call delivery.
IM	Instant Messaging	Provides 'chat' capability from PC to PC. A medium targeted between email and telephone. Often linked to Presence Awareness where staff can see if other staff are on-line and available.
UC	Unified Communications	Integration of the PC and voice services.
SIP	Session Initiation Protocol	The digital means of delivering external voice calls. More flexible and cheaper than older ISDN30 analogue connections.
DDI	Direct Dialling Inward	The range of numbers the public use to contact staff at the council
MDM	Mobile Device Management	A secure way of managing non-corporate devices such as smart phones and tablet allowing them access to council data.