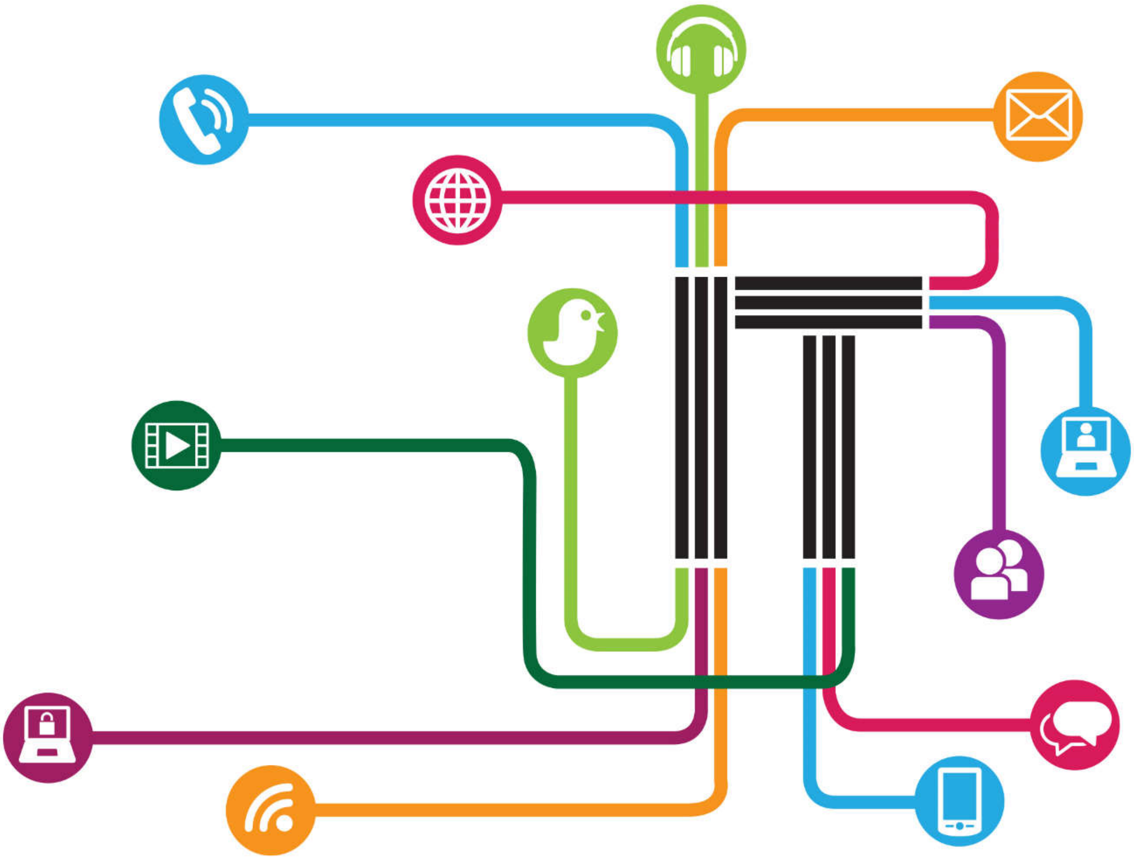

Corporate Technology Standards

Version 2.0

Coventry City Council

Revision History

Date	Version	Description	Author
27/07/2015	0.1	Initial draft.	Paul Ward
28/08/2016	1.0	First release following review	Paul Ward
05/06/2019	2.0	Revision & 2019 Update	Adam Simmonds

Table of Contents

1. Underlying Technology Standards

To support the strategic aims of the organisation, the following technology principles have been developed. All future acquisitions and/or implementation/development of technology must be made in accordance with these.

It is essential that we find a suitable balance between standardising on technology platforms - making support easier, against, perhaps limiting or hindering our ability to innovate using newer or different technologies. Where relevant, against each of the principles below, the existing technology standard is shown. It is expected that technology will be deployed in line with these standards. However, technology will always be assessed on its merits and supporting business case for deployment to ensure maximum flexibility for the organisation alongside delivery of a robust technology environment.

Please note that where a technology is listed as the current standard (e.g. operating system), it is expected that the **current major version** is supported **plus the last two major versions** of the technology.

1.1. Open Source

Solutions based on open-source technology stacks may be considered to ensure maximum flexibility and value. However, they must be designed, delivered and implemented in a supportable and secure way. Typically, where the use of open-source components falls under a support contract with the system supplier. This is to ensure the delivery of a robust technology environment.

2. Client-Side Technology

These principles cover the technology that is used on end user devices.

Browser based	All systems should be able to be accessed via a browser or thin client technology
Browser independent	Systems should be compatible across multiple browsers. **Current Standard**: Microsoft Internet Explorer & Google Chrome
W3C Compliant	All systems should be fully W3C compliant, not use any proprietary technologies and adhere to accessibility standards.
Support MSI Packaging and deployment	Where desktop deployment is required, systems must be able to be packaged into an MSI and deployed remotely Current Standard: MSI Package, deployable via Microsoft System Center Configuration Manager
Support "on-demand" or remote desktop deployments	Where desktop deployment is required, systems must be able to be packaged into an MSI and deployed on "click to run" demand by a user. Multiple thin client technologies should be supported. **Current Standard**: Microsoft Virtual Desktop Infrastructure technologies
Operating system compatibility	Systems should be compatible across multiple client operating systems. **Current Standard**: Microsoft Windows
Office tools desktop environment compatibility	Systems should be compatible with industry standard Office tools desktop environments. **Current Standard**: Microsoft Office & Microsoft Office 365
Proactive roadmap	All systems must have a proactive roadmap which demonstrates an ability and commitment to keep up to date

	with technology trends, standards and compatibilities (compatibility with **current major version minus 2** will be required)
Bandwidth/Data Transfer	Data transfer between the client tools, devices and backend databases and/or other systems must be optimised to make the most efficient use of network bandwidth. Where relevant and required, data transfer must be encrypted by default to a sufficient security level.

2.1. Bring Your Own Device (BYOD)

Currently, the majority of end user IT Equipment is provided by ICT & Digital aligned with the IT Strategy and technology provisions set out in this document.

BYOD is possible for mobile devices providing they meet and are managed by our security policies and tooling.

2.2. Mobile and Portable Device Specification

These principals and specifications build on top of those mentioned above but are specifically relevant to Mobile and Portable Devices.

Mobile Apps – Operating System	Any mobile applications must be supported across all major mobile device platforms (in particular Android). **Current Standard**: Android 8.0 (Oreo)
Mobile Apps – Device Management	Mobile applications must be compatible with mobile device management solutions **Current Standard**: • Microsoft Intune – Mobile Device Management • Microsoft Intune – Mobile Asset Management (BYOD) • Samsung Knox

For reference, below details our current standard mobile phone offering, all **new** device builds will conform to this standard:

Operating System	Android 9 (Pie)
Make / Model	Samsung J6
Device Management	Samsung Knox Microsoft Intune (MDM or MAM)

NB: Devices outside of the above specification are considered on a per-use case basis, factoring in ongoing support overheads as well as technology debt

2.3. 'Traditional PC / Desktop' Specification

For reference, below are details of our current standard desktop specification/build, all **new** computer builds will conform to this standard:

Operating System	Microsoft Windows 10 (1809) Release Channel: Current Branch*
Processor Type	64 bit
Encryption	Microsoft BitLocker
Office Tools	Microsoft Office 365 ProPlus (Click to Run) (32 Bit)

	Release Channel: Semi-Annual Channel*
Anti-Virus	McAfee Endpoint Security v10 (or newer)
Web Browser	Microsoft Internet Explorer 11 & Google Chrome

It should be noted that at the time of writing Windows 10 (1709) is deployed across the estate, but any new devices will be Windows 10 (1809). There are no plans to upgrade the existing estate from 1709, to 1809 or newer. They will be upgraded though a hardware refresh programme.

Office 365 ProPlus is the click to run of the office desktop application suite included in the Office 365 product suite. This is licensed per user and does not grant down grade rights, thus the ability to use perpetual or per-machine licensed versions. Therefore, it is effectively running an evergreen version follows the release channel above.

*Additionally, some devices will run Windows insider or Office 365 ProPlus targeted builds as part of testing for future upgrades and releases. These are limited to ICT Staff and a group of pilot users across the estate.

3. Hosting (Solutions & Infrastructure)

Wherever possible, the Council will procure cloud-based solutions and infrastructure to take advantage of:

- Rapid deployment times
- Simplified support and maintenance
- Greater scalability

Cloud based applications will be evaluated using the same criteria as traditionally “on-site” hosted applications.

In cases where this is not possible due to organisational direction, security, integration or financial reasons, the following criteria will apply:

Virtual Server Environment	Systems must be able to be hosted on Virtual Server technologies. **Current Standard**: VMWare and Microsoft Hyper-V
Operating System Independent	Systems must be able to be hosted on multiple server operating system environments. **Current Standard**: Microsoft Windows Server
Database Independent	System databases must be able to be hosted in clustered as well as standalone database environments. They should be compatible with multiple database platforms. **Current Standard**: • Microsoft SQL Server • Microsoft Azure SQL Managed Instances • Microsoft Azure SQL(PaaS)
Hardware Independent	Systems must be compatible with all industry standard hardware environments **Current Standard**: Wintel based architecture
Web Server Technology	Where systems require web server technology and are hosted on premise, this must be provided via a supported industry standard web server technology. **Current Standard:** Microsoft IIS

Support load balanced deployments	Systems must be able to be deployed into a load balanced environment using both physical and virtual load balancing appliances. **Current Standard**: Loadbalancer.org and Azure Load Balancing
Monitoring - Availability	Systems should be compatible with remote monitoring tools **Current Standard**: • Servers: Microsoft System Centre Operations Manager via locally installed agents (preferred) or SNMP. • Networking: SolarWinds (via SNMP)
Monitoring – Security	Systems should be compatible with remote monitoring, log analysis and SIEM tools.
Networking	Solutions must support and be compatible with an IP layer 2 and/or 3 network using both EIGRP and OSPF routing protocols. Solutions must also support QoS and EtherChannel technologies and be compatible with a 10 Gbps network backbone.

4. Integration & Data

These principles cover how our technology should integration and how it handles our data.

Open standards	Systems must offer supported integration techniques which can be achieved using open standards-based tools, technologies and techniques.
Adaptors provided	Systems must provide open standards-based adaptors and APIs to enable integration. Web services are the preferred method and must be supplied with a sufficient level of documentation. Adaptors must provide a sufficient level application functionality – preferably 50% - 80%.
Access to all data	All system data must be able to be fully accessed, interrogated extracted to an independent data warehouse. Data schema documents must be provided.
Data retention & disposal policies	Systems must have the functionality to be able to apply data retention and disposal policies including methods for the removal of data once retention periods have been reached. Inclusive of functionality of education, obfuscation and right to erasure (in line with data protection legislation) where appropriate.
Document storage	Where systems are required to store documents, they must be able to integrate to Electronic Document Management Solutions. **Current Standard:** • Northgate Information at Work • Microsoft SharePoint Online
Encryption	The system must be able to store, process and transfer data in a secure way i.e. with appropriate encryption and integrity checks.
Automation	Systems must provide the ability to extract and transfer data to/from other systems via automated means. This may be on-demand or via a schedule

These principals, in practical terms means that the system must allow for data to be exchanged in a automated fashion with external data warehousing and reporting tools, via use of open standards, web services, APIs and/or adapters. For reference below outlines our current data warehousing, reporting and integration stack:

NB: Preferred option is in bold

Integration Platform	**SQL Server Integration Services** BizTalk Microsoft Azure LogicApps
Reporting Platform	**PowerBI On-Premise / SQL Server Reporting Services** **SQL Server Analysis Services via Tabular Models** PowerBI Online Business Objects (being phased out)

5. Technology Adoption
These principles cover how we adopt, develop and deploy technology solutions

Stable and timely version	Technology will only be adopted and deployed to proven stable versions that are in general release from suppliers Where new foundation of supporting technology is released (such as operating system or office tools etc.) it is expected that vendors will be able to supplier a stable, fully tested version of their technology within 3 months of the release of the foundation or supporting technology.
Regular security updates	Technology adopted must be continually updated to ensure it remains secure. Where support has been discontinued, the product must be decommissioned.
Support availability	Technology deployed must have robust support arrangements in place with either suppliers or support partners. Where relevant this may include the need for 24/7 support arrangements to be available. Where relevant, solutions must support a “maintenance mode” or the ability to limit user access to the solution whilst support activity is undertaken,
Configuration & Development options	Where relevant, technology must be able to be configured and/or developed in a supported manner by Coventry City Council staff without the need to engage suppliers.
Fully tested	Suppliers must demonstrate that their solutions are fully tested for any defects. They must also demonstrate a commitment to on-going testing as they develop their product.
Production & Non-Production Environments	Technology, hosted on premise or cloud, must provide both production (live) and multiple non-production (test, training and development) environments. This must be able to be configured independently but have solutions to be able to migrate configurations between them. As a bare minimum there should be one production and one non-production environment with the preference being one production and 3 non production environments.
Remote Access	Remote access for employees will be provided via corporate devices using Microsoft Direct Access (migrating from existing solution as computers are replaced).

	For suppliers the current standard is a mixture of AppGate and Site to Site VPN. The use of browser based remote access is only permissible in exceptional circumstances and where explicit approval has been sought from the ICT Security Team. Where browser-based access has been approved it will be employee/ICT mediated and monitored access via WebEx or GoToAssist. Where third parties are accessing solutions for support, they must comply with Coventry City Council ICT Acceptable Usage Policy, relevant standards and procedures including change management.
Change & Release Management	Suppliers must provide fully documented releases for solutions. This must include the contents of the release, reasons for the release, pre-requisites, steps for how to implement, and back-out plans. Releases must comply with Coventry City Council ICT Change protocols and standards.
Bespoke Development or Customisation	Bespoke development and extensive customisation of commercial off the shelf products should be avoided. In the limited cases where this is required, supplier must make provision for these developments to be included in the standard support arrangement for the product.

6. Security

These principles cover the security expectations our technology should meet

Identity Management & Authentication	Technology must offer robust user authentication methods. Where a system is made up of multiple components or modules there must be a single authentication method covering the whole solution. Where possible technology must support single sign on with the Council's existing identity platforms and should include standards based automation to provision and deprovision accounts. **Current Standard:** • On-Premise: Microsoft Active Directory Domain Services (Kerberos or LDAP) • Cloud/Hosted: Azure Active Directory (SAML)
PSN Code of Connection (CoCo)	Where relevant, solutions must be able to support the requirements of the PSN Code of Connection
PCI SSC Data Security Standards	Where relevant, solutions must comply with the PCI SSC Data Security Standards.