



NETWORK AND TELECOMS STRATEGY

SUMMARY

- 1.1 The Network and Telecoms Strategy outlines a strategic direction and programme of work focussed on the modernisation and rationalisation of the Council's network and telephony provision.
- 1.2 The Strategy sets out to address the challenges set through the Council's transformation agenda – New Ways of Working and the ongoing drive for efficiencies, along with the national agenda, particularly around social inclusion and expanded connectivity aspirations.

RECOMMENDATION

- 2.1 To approve the Network and Telecoms Strategy.

REASONS FOR RECOMMENDATION

- 3.1 The approval of the strategy is a key decision

SUPPORTING INFORMATION

- 4.1 The Network and Telecoms Strategy is included at Appendix 2.
- 4.2 The scope of the Strategy covers:
 - data over local and wide area networks
 - voice, video and teleconferencing
 - wireless, including private and public access networks
 - mobile and home working solutions
 - partnerships and shared services opportunities
 - secure services for exchanging classified information with central government, health, criminal justice and other agencies through Government Connect.

4.3 The first phase of this modernisation programme has now been completed:

- the appointment of a Head of Strategic Infrastructure
- the award of a telecommunications contract to reduce our call costs, with a projected saving of £90k per annum on call charges
- the deployment of a new Voice-Over-IP - VOIP - a unified data and telecoms network system to around 1000 employees, funded by savings through reductions in our BT FeatureNet estate
- ongoing reviews of mobile phones, FeatureNet, Access Circuits and other rented services saving in excess of £40K per annum and a one-off recovery of over £20K from BT
- functional review of the Derby Direct contact centre
- integration of telecommunications into the new IT FM service
- alignment of Council networking provision with Children and Young People and Building Schools for the Future
- completion of the first phase of the city centre - Cathedral Quarter, wireless networking project with free Internet access in the Market Place for Library card holders.

4.4 The future phases of this modernisation programme are covered in the action plan within the Strategy.

OTHER OPTIONS CONSIDERED

- 5.1 Opportunities for shared services have been and will continue to be considered for the development and provision of the Councils Network and Telecoms provision.
- 5.2 The strategy is being driven from the operational and modernisation needs of the Councils services. Full options appraisals are undertaken before any technical and/or investment decisions are considered.

For more information contact: John Cornall 01332 255334 e-mail john.cornall@derby.gov.uk
Miles Peters 01332 256268 e-mail miles.peters@derby.gov.uk
Background papers: None
List of appendices: Appendix 1 – Implications
Appendix 2 – Network and Telecoms Strategy

IMPLICATIONS

Financial

- 1.1 The action plan to deliver the Network and Telephony strategy will be underpinned by individual business cases, identifying both investment and savings requirements.

Legal

- 2.1 None directly arising.

Personnel

- 3.1 None directly arising

Equalities Impact

- 4.1 An Equalities Impact assessment will be completed as part of the Strategy. One area of particular note will be around social inclusion.

Corporate objectives and priorities for change

- 5.1 Increasing economic growth and sustainable investment.

DERBY CITY COUNCIL

A 21st Century Network for a Connected Derby

A Telecoms and Network Strategy

Version: 4.0

CONTENTS

1. Vision
2. Current Network and Challenges
3. The Transformation Drivers
4. Strategic Road Map and Objectives
5. Key Risks and Dependencies
6. Glossary
7. Action Plan
- A. Appendix A

1. Vision

For Derby to have a 21st Century Council network supporting high quality delivery of council services and positively supporting the ongoing transformation programme.

The Council's Network will:

- have appropriate and reliable availability and quality of service.
- be scalable to readily accommodate changing requirements.
- be sustainable and have a clear focus on delivering ongoing efficiencies.
- be secure in terms of accessibility, data integrity and information confidentiality.
- provide for 'Intelligent working' to support the Council's Transformational Programme – 'Transforming Derby'.
- be closely integrated and coordinated with the Accommodation and Customer Service Strategies.
- be based around a single protocol, standards based IP Network Infrastructure.

This strategy will cover the following networks:

- Data
- Voice
- Video
- Mobile
- Remote
- Wireless

With coverage including:

- DCC Core network
- DCC Schools network
- DCC Home users
- DCC Remote users
- Shared occupancy sites
- Partners
- Shared services consortiums

2. Current Network and Challenges

The DCC network is a complex one, connecting over 150 sites using a number of technologies. It has grown and developed incrementally, and whilst functional it has become somewhat fragmented, becoming increasingly inflexible and costly to maintain.

To meet the challenge of providing an efficient and effective 21st Century network there are a number of unique areas which must be addressed:

- local networks
- wide-area networks
- voice networks
- wireless networks
- mobile networks.

Appendix A summaries the current position across the council, on all these networks, along with an indication of the challenges we face. The strengths and weaknesses of the network are summarised in the next section.

Strengths

- Core network has no current capacity issues. The core switches have been recently upgraded.
- Distribution network (LES and EES) is now quite extensive and ripe for exploitation by services such as building management, CCTV and most importantly telephony and video conferencing, to support new ways of working and to offset the increasing revenue costs.
- Access network is partially upgraded, the VOIP project made a substantial investment in replacing all access switches.
- Have access to good technological solutions through our Technology Partners.

Weaknesses

- Access network still has a sizeable number of obsolete switches.
- The network configuration needs substantial rework to allow the investment in new infrastructure to realise improvements in reliability.
- The fixed voice network is fragmented, one quarter is new and versatile, one half is old and inflexible but cheap to run, and one quarter on Featurenet is both old and expensive to run. The business case to modernise the phones only extends to the Featurenet legacy estate on the MAN network – the WAN network does not currently support VOIP.

- The security model for accessing corporate applications requires all assets to be DCC owned and managed. There is great difficulty in making our applications available to users outside our network and web publishing has been limited.
- Difficulties in catering for the home office user, with a DCC laptop and broadband service.
- Limited success in delivering applications to DCC users operating from third-party networks, for example Adult Services staff at the Lighthouse, where the PCs and network are operated by Derwent Shared Services.
- Difficulty giving non-DCC staff access to their own organisation's services, for example Derbyshire CC staff working within DCC.
- Applications increasingly managed remotely, Academy, [Anite@Work](#), Exor, Selima, Chipside, requiring third-parties to remotely access internal network resources. A third-party Demilitarised Zone - DMZ – a zone on the network between the internal secure network and the internet for public-facing services is an unsustainable workaround as 13 of 16 network interfaces on the firewall are now fully used.
- The old approaches to securing the network perimeter is rapidly becoming obsolete. The demand for new services including voice, video and teleconferencing requires new approaches to securing our network.
- Firewalls are increasing ineffective against modern threats. Integration with remote applications using web services requires significant investment in “layer-7” filtering, employing a new class of firewall with application intelligence.
- Web publishing with Microsoft Internet Security and Acceleration Server - ISA server - has proved problematic. Not all applications lend themselves to the web approach, and not all third-party developers write code well enough to be published. This has led to often costly workarounds being adopted.
- There are issues relating to compliance with Government Connect Code of Connect - CoCo - for home working, to be sustainable there needs to be a minimum of 50 home workers to engage the appropriate broadband contract.

3. The Transformation Drivers

3.1 Supporting the Corporate Plan

Effective communications are fundamental for the council to be able to deliver the Council's priorities for improvement.

- Making us proud of our neighbourhoods.
- Create a 21st Century city centre.
- Leading Derby towards a better environment.
- Supporting everyone in learning and achieving.
- Helping us all to be healthy, active and independent.
- Give you excellent services and value for money.

To be able to deliver effective communication now, and moving forward to deliver against the future changing requirements will require a modern, flexible and sustainable network infrastructure. The network infrastructure will need to support and be closely coordinated with:

- The Council's Accommodation Strategy.
- The ongoing drive to deliver real tangible efficiency savings including energy efficiencies.
- The Customer Service Strategy and the developing requirements of our citizens and their neighbourhood.
- The drive to identify and deliver shared services opportunities with partner organisations.
- The Building Schools for the Future - BSF - Programme and the development of personalised learning.
- The Council's Equalities Commitment and the Wider Social Inclusion Agenda.
- The Workforce Development Programme particularly around flexible working.

3.2 Responding to Internal Challenges

The Council also faces a number of specific technical challenges:

- The growth in the number of servers reflecting the demand for new applications. The current estate has doubled in size to 200 servers, from 100 three years ago.
- The growth in the complexity of configurations. The largest systems three years ago were Swift (Social Services), Orbis (Revs and Bens), Coda (Finance), each on a single server. Swift now includes the Electronic Social Care Record - ESCR - and Integrated Single Assessment (ISA) having 9 servers in total, The Oracle 11i replacement for Coda has 6 servers, and the DCC Customer Services Information System - CSIS -, an entirely new system and is dependant on at least 15 servers.

- The local area network - LAN - growth connecting sites. When first created seven years ago there were 4 sites, there are now 26 sites on the DCC LAN, and over 100 on the Schools LAN. The busiest core switch then had 12 switches connected, it now has 83 switches connected.
- Growth in the use of the Internet for connectivity. Three years ago there were no Virtual Private Network -VPN - sites, now there are 18, and over 60 remote-access users.
- Deployment of new network services including Internetwork Protocol Telephony - IPT -, video web-casting and conferencing, building management, physical security, CCTV, wireless and fixed-to-mobile converged services and presence-awareness.
- Growth in Internet Presence.
- The main voice network system is nearly 18 years old and there is a significant capital cost hurdle for connecting smaller sites.
- The requirements of the development and growth within Derby Direct is pushing the limits of the contact centre telephony system.
- The FeatureNet contract has a low capital but high revenue cost (high long term cost of ownership).
- Piecemeal coordination and management of mobile contracts, Vodafone with 100 handsets and Orange with 835 handsets, all mostly voice and Short Messaging Service - SMS -, with some 3G and push e-mail.
- Rising expectations of users, demanding web conferencing, use of their own broadband at home, making more and more exceptions to the rule.
- Accommodation moves and changes, poor planning and communications, slow to implement, network provisioning dictated by BT's responsiveness Enterprise Extension Service - EES - orders could take 4-5 months to be fulfilled).
- Asset tracking, equipment, personnel, active Radio Frequency Identification - RFID - tags, mobile stations in vans etc.

3.3 Responding to External Challenges

The organisation is also increasingly affected by external forces, with the evolution of shared-site operations and shared services with partners, impacting on our security policy. The organisation once had complete control of a single security policy, but this is no longer the case:

- DCC network, with increasing demand to modify security policies to enable services, creating further exceptions to manage.
- DCC schools network, where the BT managed LAN encroaches upon both DCC services such as the Oracle FMS, the DCC “admin-PC”, the “admin-network”, and curriculum networks.
- DCC partnership networks (such as Derwent Shared Services facilities in LIFT and REVIVE and libraries application network hosted by Derbyshire County Council), where the partners security policy must be accommodated
- N3 access network – the private network used by the Health Service, subject to the N3 code-of-connection security policy, particularly in co-location offices such as Beaufort Street where health workers share facilities.
- The Government Connect challenge is the most important, to be able to continue to fulfil our statutory obligations we must conform to the code of connect. We must re-establish central control of security and extend the perimeter of control to all locations requiring access to GSi resources. This will include revenue and benefits access to DWP Customer Information System - CIS -, social care functions including secure email through N3 and criminal justice access to Libra, the Criminal Justice IT - CJIT - case management system.

3.4 Responding to External Opportunities.

DCC is involved in a number of city-wide initiatives to develop network connectivity and services, or potential collaborations:

- Litespeed, the 21-Century Derby project to develop a public-access fibre-optic network across development areas in the city.
- Collaboration with Derby University and Derby College for shared network access across the City Centre wireless network.
- Collaboration with the Building Schools for the Future – BSF – Local Education Provider - LEP - to provide access to the Schools network at neighbourhood level using wireless technology.

4. Strategic Road Map and Objectives

4.1 Objectives

The overreaching strategic objectives to deliver a 21st Century connected network for Derby are –

- 1 Deploy a modern, sustainable unified communications network delivering integrated voice, data and mobile services.
- 2 Develop the case for deployment of a city wide wireless network.
- 3 Establish a single desk top support service for IT and Telephony.
- 4 Develop a communications network to support flexible working including home, mobile working and 'hot desking'.
- 5 Develop the infrastructure capability to share network services across partner organisations throughout the city and region.
- 6 Comply with government mandatory security controls such as the GCSx code of connect.
- 7 Ensure the Council's network is developed to be fully compliant with Government Connect CoCo.

All underpinned by an overriding objective to ensure value for money.

5. Risks and Dependencies

5.1 Risks

- DCC requirements are not fully coordinated, leading to gaps in provision and needless expense in provisioning services in an unplanned reactive manner.
- Market failure leading to exploitation by British Telecom – the broadband networks, with the exception of NTL, are delivered over BT infrastructure. This is already an issue, BT increased prices on EES circuits at extremely short notice, leading to 140% price rises across the C&YP Schools Network, making the provision unaffordable.

5.2 Dependencies

- Consolidation of departmental budgets for telecoms, network and mobile to permit consolidated tender and contract award to achieve the best possible value.
- Governance over procurement of telecoms, network and mobile services to avoid dilution of the benefit of consolidated contracts.

6. Glossary

Access Network	the switches and cabling making up an office network, to which PC's and telephones are connected, to access central services
EES	Enterprise Extension Service provided by British Telecom, a high speed network link used by us to connect local area networks at larger offices around the city
FeatureNet	a telephone service provided by British Telecom, a legacy of the Derbyshire County days. Each handset is rented at an average cost of 150 a year, and tied to an expensive contract for making calls, about double the call rates of our new KCOM carrier
Government Connect	the secure private network for Local Government to communicate securely with central government, health, the police service and criminal justice services. DCC must join the network to continue to receive information from DWP. Joining the network has stringent obligations outlined in the Code of Connect (CoCo) document to ensure security. These measures are onerous and do require substantial revision to our infrastructure and operating procedures
IP	Telephony or VOIP (Voice over IP) – a technology for making and receiving calls over the data network, usually sharing the same connection as the user's PC
LAN, MAN and WAN	the LAN (Local Area Network) is made up of switches and cabling which we own ourselves, nothing is rented, and the cabling is mostly confined to our premises, though we do have some cabling under the market square, several radio and one laser link. The MAN (Metropolitan Area Network) is a fibre optic network, some we rent from KCOM to connect our main buildings, the majority being British Telecom fibre links making up the remote office and schools network, and the Cable and Wireless circuits linking us to Serco's data centre in Birmingham. The WAN (Wide Area Network) is made up of routers and links via BT to distant locations and to the internet

N3	the secure private network for health providers and practitioners. We already connect to local health provider networks for exchanging information. however this is an ad-hoc local arrangement and the approved method is via Government Connect, onto the government secure intranet (GSI), which in turn links to N3. Secure communications with health are essential in fulfilling social care functions
VPN	Virtual Private Network, a technology to use the internet or third-party networks to securely access our own network remotely. Members use VPN services for home access. The Government Connect CoCo requires us to implement a new and more secure system for VPN access

7. Action Plan

Activities	Objective	Outcome	Responsibility	Target Date	Achieved Date
Data					
Review of the council-wide network infrastructure	Identify efficiency and modernisation opportunities	Reduce cost and deliver more effective solutions	Head of Strategic Infrastructure	Ongoing	
Accommodation network planning	Ensure alignment with the Accommodation Strategy	Telephony and Network requirements and infrastructure are integrated within the Accommodation reviews/strategy	Assistant Director of ICT and Procurement	Ongoing	Ongoing
Voice					
Build in Telephony support to the standard desk top support function		To build in the requirement of a single desk top support service within the new ICT FM Contract, covering both desk top completing and telephony	Head of Strategic Infrastructure	01/11/08 (Linked into the ISOS process)	12/12/08

Activities	Objective	Outcome	Responsibility	Target Date	Achieved Date
Phase 1 of Transfer FeatureNet to Cisco	Cost reduction Feature enhancement	Remove 1000 FeatureNet lines at Heritage Gate and other EES connected sites (excepting St Mary's Gate) Achieved 1230 reduction	Head of Strategic Infrastructure	31/07/08	23/09/08
Phase 2 of Transfer FeatureNet to Cisco	Cost reduction Feature enhancement	Replace 600 FeatureNet lines at St Mary's Gate and new / deferred EES connected sites	Head of Strategic Infrastructure	01/12/09	
Derby Direct Functional/Capacity Review	Solution mapping and contribution to business case	To review the functional requirements and growth plan for Derby Direct and determine appropriate telephony options a) Limited upgrade to current Mitel system b) Possibility for an externally hosted service c) Mitel replacement	Head of Strategic Infrastructure and Head of Customer Service	31/10/07	01/09/08

Activities	Objective	Outcome	Responsibility	Target Date	Achieved Date
Business Case for Contact Centre platform upgrade or replacement	Facilitate procurement	Business case for upgrade or replacement	Head of Customer Service	01/09/09	
Video					
Community Safety Partnership wireless CCTV platform	Mobile CCTV capability	Facilitate CCTV in neighbourhoods	Crime Prevention Team leader CSP Head of Strategic Infrastructure	01/04/08	04/03/09
DCC CCTV fixed and wireless digital enablement project	Sustainable fixed CCTV capability	Assist in DCC digital conversion of CCTV network exploiting DCC converged data network – including use of public realm wireless mesh	Traffic Manager Head of Strategic Infrastructure	Pilot 01/06/09	
Teleconferencing and telepresence project	Teleconferencing facility	Voice, video and data sharing online conferencing capability within DCC and with partners	Head of Strategic Infrastructure	01/12/09	

Activities	Objective	Outcome	Responsibility	Target Date	Achieved Date
Mobile					
Consolidate the Council's mobile phone contracts and establish a governance framework for ongoing management and control	Single contract	Reduce costs and maximise control and recovery of personal usage.	Head of Strategic Infrastructure	01/09/09	
Remote					
Home Working Project	Sustainable home working solution	To ensure that the Telephony and Network requirements for the Home Working Project can be delivered	Assistant Director of ICT and Procurement	Ongoing	Project subsumed by NWoW
Replacement mobile email and data solution	Achieve Manual V compliance	Allow mobile devices to handle restricted or sensitive email (unlike current solution)	Head of Strategic Infrastructure	01/09/09	

Activities	Objective	Outcome	Responsibility	Target Date	Achieved Date
Wireless					
Development of Public Realm wireless capability	Exploitation of the network	Multiple services including CCTV being delivered on the infrastructure to achieve sustainability	Head of Strategic Infrastructure	Ongoing	
Consolidation of existing wireless	Achieve Manual Y compliance	Secure and maintainable wireless capability	Head of Strategic Infrastructure	01/09/09	
Security					
Achieve and maintain Government Connect CoCo compliance	Maintain our link to DWP and any other GSi resource as required by the business	Secure and connected network to Central Government	Head of Strategic Infrastructure	Exemption 01/04/09 Compliance 01/09/09	

Activities	Objective	Outcome	Responsibility	Target Date	Achieved Date
Shared Services					
Deliver new network access solution to facilitate multi-agency working	To facilitate shared services	Shared services can be achieved in multiple-occupancy offices	Head of Strategic Infrastructure	01/12/09	
ICT Component of the Building Schools for the Future Programme		To deliver a high level strategic statement for ICT within the BSF Programme and provision of going support to the BSF Programme	Assistant Director of ICT and Procurement	30/09/07	16/08/07

Appendix A

A.1 The Metropolitan Area Network (MAN),

This is a high speed network connecting our main sites, made up of a number of elements;

- The core network comprising of four nodes, at the Wyvern (at Capita's Mallard House, to be moved to Serco's Salisbury House), Middleton House, Roman House and the Council House. The data centre, when relocated to Birmingham in April will be connected by a pair of similar high capacity circuits to Salisbury House and the Council House.
- The distribution network, running over BT EES point-to-point fibre-optic links, radiating out from Middleton, Roman and Council House switches, to medium sized offices. These circuits are contracted by the council and managed by the DCC FM provider. The network is scalable and reliable, but with recent major price rises from BT, becoming prohibitively expensive to extend to smaller offices, as well as more than doubling our rental costs.
- The schools distribution network, connected to Roman House and Middleton House, linking to Ashgate and Ravenscroft schools, and then to primary and secondary schools in the City. These are contracted from and managed by BT global services, which has implications in that the circuits tied to the overall BT management contract. It is likely that the Building Schools for the Future - BSF ICT partner will wish to change the disposition of circuits, which due to the tie-in to the BT contract, will incur re-provisioning costs.

The technologies used by the MAN allow any number of sophisticated network services to be delivered, including voice, video, cctv, building management, telepresence and fixed to mobile integration. The exception though remains the schools network which lies outside corporate management and governance, which for security reasons, cannot benefit from the range of services we are able to deliver over the MAN.

A.2 The Wide Area Network (WAN)

The wide area network connects smaller and more remote sites to the network core, comprises a mixed estate of largely legacy technologies, with many of the circuits having been provisioned over 10 years ago:

- BT MegaStream and KiloStream private circuits, mostly connecting Social Services sites at much lower speeds. DCC had been replacing these circuits with BT EES, to reduce revenue costs and gain better performance, until BT raise prices, effectively ending the existing business case to upgrade.

- Private Broadband networks. Schools used to be connected by one of two operators, East Midlands Broadband Consortium (EMBC) with their Local Loop Unbundled (LLU) symmetric broadband network operated by Kingston Communications/ Affiniti, and BT IP Stream, using the BT asymmetric broadband solution. The former proved to be an extremely costly solution and recently was decommissioned, migrating these schools to the new BT EES network. The latter has been retained as a backup for the schools network, as well as being deployed to a small number of SureStarts.
- Public Broadband network, business and domestic broadband. Small sites are being connected using site-to-site Virtual Private Networking (VPN), and lone and home workers using client VPN. This is costly when the Internet service provision at the “DCC-end” is factored in, and is typically very unreliable and problematic to support. Fundamental to this is the fact there are no service guarantees.

A.3 The Wireless Network

Wireless networking has become a major area in the past two years, needing its own infrastructure and strategy. Developments include

- The security challenge presented by Government Connect requires us to overhaul the existing “in-building” provision with much tighter security and policy management. Non-compliant access points will need to be replaced and measures put in to ensure end-user introduced access points are detected and disabled.
- Implementation of site-to-site connections using wireless technology, primarily in schools to minimise circuit rental costs, but anticipated in other areas such as highly secure links between the magistrates court to St Mary’s Gate to delivery CJIT systems access.
- Implementation of outdoor wireless access in the City Centre, allowing the public to access the Internet if they hold a library card and a range of DCC services including laptops, mobiles and CCTV cameras.

A.4 The Fixed Voice Network

The voice network is diverse, with approximately 4000 handsets, on four platforms:

- DCC-owned Cisco Unified Communication System - UCM. The new and preferred platform for voice-services, and using the data network as its transport. This is a modern IP-telephony system well placed to support New Ways of Working, and deployed to 940 users across approximately 12 sites. Deployment to a further 700 users, principally to St Mary’s Gate is planned for the second half of 2009. The

deployment of 550 devices to the council house and 300 devices to the decant location is on hold.

- DCC-owned Mitel voice system. This is the legacy Mitel SX2000 switch, installed at the Council House in 1989 and gradually extended to 10 sites. The network operates over its own copper wiring with WAN links or access circuits, rented from BT, and is entirely separate to the data network. The Derby Direct contact centre operates on IP-telephony extension of this platform. About 1700 users in total.
- BT FeatureNet system, rented under a restrictive contract. renewed each December. It is largely a legacy of the old Derbyshire County Council presence in the city and is retained across the majority of smaller offices where data network provision is limited. About 1100 users remain.

The network strategy instigated the first phase of a project to modernise the voice network, resulting in the implementation of the Cisco UCM system, deploying 940 phones and replacing and rationalising 1280 FeatureNet lines.

A.5 The Mobile Network

The mobile network is fragmented and poorly controlled:

- The “Official” mobile voice contract was awarded to Vodafone and costs are based on the G-CAT catalogue. DCC presently have nearly 760 handsets, almost without exception these are simple voice and SMS devices. To minimise fixed-to-mobile costs a Vodafone “Virtual Fixed Link” has been implemented, significantly reducing the cost of calling from Cisco, Mitel and FeatureNet phones.
- Unofficial procurement arrangements have been in place with Orange for some years following Commercial Services decision not to procure through the corporate contract, later joined by C&YP. There are in excess of 987 handsets. These are mostly paid by variable direct debit let under 21 separate contacts with a monthly spend exceeding £10K
- Implementation of mobile data services, based on GSM/GPRS and UTMS/3G technologies, for the remote DCC worker have been conducted in a piece meal manner without consideration given to security or engaging private network services from the carriers. Current implementations use the Internet as an intermediate carrier and secure the connection by remote-client VPN. This is appropriate for small numbers of users but will prove costly and complex to administer in larger numbers.

A moratorium has been enacted on procurement outside of the corporate contract, save for specialist devices better supported on Orange, in preparation for a tender under the new OGC framework.

A.6 Managing Security

The DCC network at present does not distinguish between shared assets, (i.e. Infrastructure domain controllers , file servers, access servers and application servers database servers and other shared computing devices), and user devices (pc's, laptops, mobiles, kiosks, projectors). This is not an issue where the network is small and manageable, with a single security policy, and all devices within the network under central control.

However, the DCC network passed beyond this realm several years ago, with deployment of an extensive schools network with devolved control, with development of shared office working with partners, with peering and transiting arrangements across the network with other parties, and with an increasing Internet presence.

The network is now too large and too complex to manage successfully under one security policy. The current policy, where it is not bypassed entirely, is now becoming too restrictive to accommodate new business needs.

The most significant challenge lies with the fact the network cannot meet mandatory requirements for accessing Central Government Services on the Government Secure Intranet – GSi through access provided to Local Government by Government Connect – GCSx. To achieve compliance it has been necessary to build a separate restrictive network within the Council House to allow benefits staff to access the DWP Customer Information System CIS, to allow DCC to continue to pay housing benefits.

This deployment is tactical and limited in scope, as the obstacles to compliance are fundamental and wide ranging and require corporate governance over the network. Government Connect have stated they require us to extend the boundary of control to our entire network for us to retain any interim short-term approval they might grant us to maintain our link.

A.7 Making Services available on the Internet

When the DCC network was first conceived, there was little if no requirement for DCC to have an Internet presence. To deliver the small requirement a single firewall was implemented, creating a separate security zone for the small number of assets required. A De-Militarised Zone (DMZ), a zone where the DCC security policy was relaxed to allow “outsiders-in”.

The DCC Internet presence has since grown significantly, and the single DMZ has grown to four DMZ's, with nearly thirty servers within the zones. As the size and criticality of the services delivered over the Internet has grown so has the need to significantly improve security within the zones as the threat of hacking too has grown. The firewall itself is now incapable of protecting against all threats, and additional tactics such as implementing an Intrusion Detection System (IDS) and use of secondary firewalls such as ISA Server for web publishing have become necessary.

Where there was once one firewall securing the internet service, DCC now has in excess of ten firewalls, securing various ingress points into the network, including Derbyshire CC, Derbyshire Fire and Rescue, Serco, Capita, British Telecom, Affiniti, Cable and Wireless, Traffic Management, Friar Gate Studios, the Youth Justice Board and most importantly GCSx. The proliferation of firewalls, and the increasing sophistication of the threats against the network, diminishes the sustainability of firewalls as the main security solution.

A.8 Providing Remote Access

Our remote access solution, whilst workable, does not address the current remote access security requirements

Our principal client remote access solution uses Microsoft ISA Server 2004 with single-factor authentication. This is not GCSx compliant and further measures must be put in place to ensure remote access is secure for access to PROTECT or RESTRICTED information. The solution requires a technology update and the implementation of secure authentication such as smartcard or token technology.

Our mobile email solution using Microsoft Exchange 2003 and Microsoft ISA Server 2004 is not GCSx compliant and again, cannot be used for protectively market information access. Government Connect require us to demonstrate efforts to comply with the code of connect, which will require us to refresh or replace the remote access infrastructure.

One option might be to extend our Citrix access gateway solution to achieve secure remote access but this again requires implementation of secure authentication to be compliant. Citrix is not a cheap solution and this option becomes increasingly unsustainable if it is used as a principal means of access.