SUBMISSION TO THE STRATEGIC (OVERVIEW AND SCRUTINY) COMMITTEE

Date: 29 January 2014

Agenda item: 6

Contact Officers: Jane Kitchen/Kevin Sleeman

Phone: 01543 308077/120

SUBMISSION BY CLLR I EADIE, CABINET MEMBER FOR IT AND WASTE MANAGEMENT

ICT - LOOKING TO THE FUTURE

1. Purpose of the Report

1.1 The Council is experiencing a number of core challenges in relation to its use of Information Technology (IT) that need to be addressed. The core challenges are:

- The end of support by Microsoft for Windows XP and Office 2003
- The threat of disconnection from Central Government networks by the Cabinet Office.

1.2 An IT Review Group was formed following a report to the Council's Leadership Team in July 2013 and after consultation with the Cabinet Member for Finance, Democratic and Legal Service, who at the time was responsible for IT. The group comprised of the Cabinet Member responsible for IT and Waste Management, the Leader of the Labour Group and Officers from across the Council. This report provides Members with the opportunity to scrutinise the information considered by the IT Review Group and the recommendations that are being proposed.

2. Background

2.1 IT is intrinsic for virtually every aspect of the Council's business from the management of planning applications through to monitoring the collection of rubbish, the running of leisure centres and recording the condition of trees. The diagram in Appendix A shows the reach of IT across the various Council premises. Many of the Council's services have public facing elements that allow the public an element of self-service through the Council's website. Although self-service is subject to a separate Fit for the Future project, it is worth noting that:

- Between December 2012 and November 2013 there were 30,294 electronic payments made to the Council, equivalent to one every four minutes during office hours. Without the electronic payments system these payments would have needed to be made either at the offices or over the telephone.
- During the year April 2012 until March 2013 there were 273,573 searches carried out on the Council's online planning system. When comparing the period of April to August for 2012 and 2013 an additional 28,000 searches were made in 2013 compared to 2012. Without this feature available to the public it would have increased the number of enquiries made to the offices.

2.2 The Council faces challenges around the use of the software on its computers. Primarily due to the decision by Microsoft to end the support for Windows XP and Office 2003 on 8 April 2014 and the Cabinet Office disconnecting Council's from the Central Government Network in September 2014 if they still use Windows XP. Windows XP is the operating system running on the Council's desktop computers and all of the software programs the Council runs sits on top of this.

2.3 One approach could be to change the operating system for a more up to date version such as Windows 7 and Microsoft Office 2013 on the 94 out of 390 devices capable of supporting an upgrade. However, doing this would lead to other problems, such as the current version of the email software (Microsoft Exchange) needing to be upgraded as it is not compatible. The current Microsoft Exchange server is too old to support the new version so would need replacing. There are also 503 software applications that need to be evaluated as to whether they are compatible with a newer operating system. A further issue is the current Council server room that houses the majority of the servers and communications lines has been identified as having little resilience in the event of a fire. All of the issues together with recommendations to resolve them are summarised in this report:

- The implications for the end of support by Microsoft for Windows XP and Office 2003 further details are shown in Appendix B.
- What needs to happen to servers and desktops that have passed their useful life as outlined in Appendix C.
- How to ensure fit for purpose issues of the current server room is resolved as set out in Appendix D.
- Updating the Business Continuity Solution for IT to reduce the current downtime of at least 3 days should a disaster occur as set out in Appendix E.
- The implications of the threat of disconnection from Central Government networks by the Cabinet Office. See Appendix F.
- Review of the ICT Access, Use and Security Policy. Details contained in Appendix G.

3. Recommendations

3.1 To recommend the following Task Group proposals to Cabinet:

3.2 In relation to the challenge regarding the end of support by Microsoft for Windows XP and Office 2003 the following recommendations are made:

- Adopting Windows 7 as the replacement operating system to Windows XP (paragraph B.4.4).
- Upgrading to Microsoft Office 2013 for the desktop document production software (paragraph B.4.7).
- Implementation of Microsoft Lync to improve working on documents both within the Council and with other linked agencies (paragraph B.4.8).
- Developing a training programme to assist Members and Officers in moving from the current versions of the software to the proposed versions (paragraph B.4.9).
- Appointing additional resource to support the ICT team on delivering the project (paragraph B.4.11).
- Procurement of a software application to store archive information from systems that only hold historical information (paragraph B.4.12).
- Procurement of a software application to assist with training Officers in policies and procedures and identifying training needs (paragraph B.4.13).

3.3 To address the threat of disconnection from the PSN the following recommendations are made:

- Replacement of the core activity and auditing tool (paragraph F.6.1).
- Implementation of additional servers to meet the Cabinet Office requirements (paragraph F.6.2).
- The closure of Outlook Web Access and the movement of secure email boxes to a third party (paragraph F.6.3).
- Purchase and implementation of encrypted memory sticks (paragraph F.6.4).
- Implementation of additional mobile phone security to meet the Cabinet Office requirements (paragraph F.6.5).
- Undertake a programme of Verification of Criminal Records checks to comply the Cabinet Office's for the Baseline Personnel Security Standard (paragraph F.6.6).

3.4 In reviewing the ICT Access, Use and Security Policy the following recommendations are made:

- The policy in Appendix K is adopted as a Council policy (paragraph G.2.1).
- A two-stage sign off approach is adopted and all Members and Officers will sign the new commitment statement (paragraph G.2.2).

3.5 In considering the remaining issues the following recommendations are made:

- The Council adopt option C2 of those investigated by the IT review group that contains the following features (paragraph I.2.2):
  - Replacement of some desktop computers and laptops.
  - Conversion of the majority of the equipment to act as thin clients.
  - Purchase of new servers from the ANS group.
  - Placing the servers in the County Council server rooms and making use of their disaster recovery capabilities.

3.6 The outcome from implementing these recommendations is described in Appendix J.

4. Community Benefits

4.1 In delivering effective and efficient services to the Community it is essential that the Council's ICT is fit for purpose.

5. Financial Implications

5.1 The Council is unlikely to borrow specifically for ICT investment due to the asset life being relatively short in comparison to other Capital Investment projects and therefore we are likely to utilise any available resources such as capital receipts to fund this project. The overall financing of the recommended Capital Programme including the ICT investment will form part of the Medium Term Financial Strategy (Revenue and Capital) 2014-17 to be approved by Council on 24 February 2014.

5.2 The current costs of ICT to the Council are explained in Appendix I.

5.3 The costs that have been identified for implementing the recommendations are given in the table below:

Appendix	Year 1		Year 2		Year 3		Year 4		Year 5		Total	
	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue
	£	£	£	£	£	£	£	£	£	£	£	£
Investments												
B (Software)	79,370	7,240	12,400	7,380	0	7,530	0	7,680	0	7,830	91,770	37,660
F (Public Sector Network)	67,580	6,940	0	7,070	0	7,210	0	19,800	0	20,190	67,580	61,210
H (New hardware)	974,940	151,420	14,850	152,350	3,580	153,400	24,680	154,480	12,800	155,560	1,030,850	767,210
Total	**£1,121,890**	**£165,600**	**£27,250**	**£166,800**	**£3,580**	**£168,140**	**£24,680**	**£181,960**	**£12,800**	**£183,580**	**£1,190,200**	**£866,080**
Savings												
B (Software)	0	(39,990)	0	(39,990)	0	(39,990)	0	(39,990)	0	(39,990)	0	(199,950)
F (Public Sector Network)	0	(2,410)	0	(2,410)	0	(2,410)	0	(2,410)	0	(2,410)	0	(12,050)
H (New hardware)	0	(55,530)	0	(55,530)	0	(55,530)	0	(55,530)	0	(55,530)	0	(277,650)
Total	**£0**	**(£97,930)**	**£0**	**(£97,930)**	**£0**	**(£97,930)**	**£0**	**(£97,930)**	**£0**	**(£97,930)**	**£0**	**(£489,650)**
Grand Total	**£1,121,890**	**£67,670**	**£27,250**	**£68,870**	**£3,580**	**£70,210**	**£24,680**	**£84,030**	**£12,800**	**£85,650**	**£1,190,200**	**£376,430**

6. Strategic Plan Implications

6.1 By implementing the recommendations of this report it will give appropriate, robust ICT that will enable elected Members to effectively communicate with their electorate and Officers to deliver Council services thereby supporting the outcomes of the Strategic Plan.

7. Risk Management Issues

7.1 The following specific risks have been identified as relevant to this report.

Risk Description	Likelihood / Impact	Status	Risk Category	Countermeasures
Using Windows XP after the end of Microsoft support allows the introduction of viruses and malware	Significant / Significant	Severe	Technological	Implementing restrictions on the use of removable media and new firewalls should assist in containing the risk during the transition period.
That the Council has its link to Central Government IT networks disconnected	Significant / Significant	Severe	Technological	The proposed solution will be implemented using designs compliant with the Cabinet Office recommendations.
Applications are not rationalised to minimise the conversion work	Medium / Significant	Material	Technological	Information will be used from the monitoring software already in place to put together an evidence based approach to determining applications that will be converted.
Managing costs to ensure they do not exceed the budgets allocated	Low / Medium	Tolerable	Financial	A project board and governance mechanism will be established and changes to the project scope will be agreed by the project board within the tolerances set by the organisation.
Managing any changes to the contract with the outsourced ICT provider	Medium / Low	Tolerable	Legal	Representatives from the ICT provider have been involved in the project since the beginning and contractual issues discussed as appropriate.

Background Documents:

All background information is attached in the Appendices.

Diagram showing sites where ICT is located at present and the number of clients on each site.

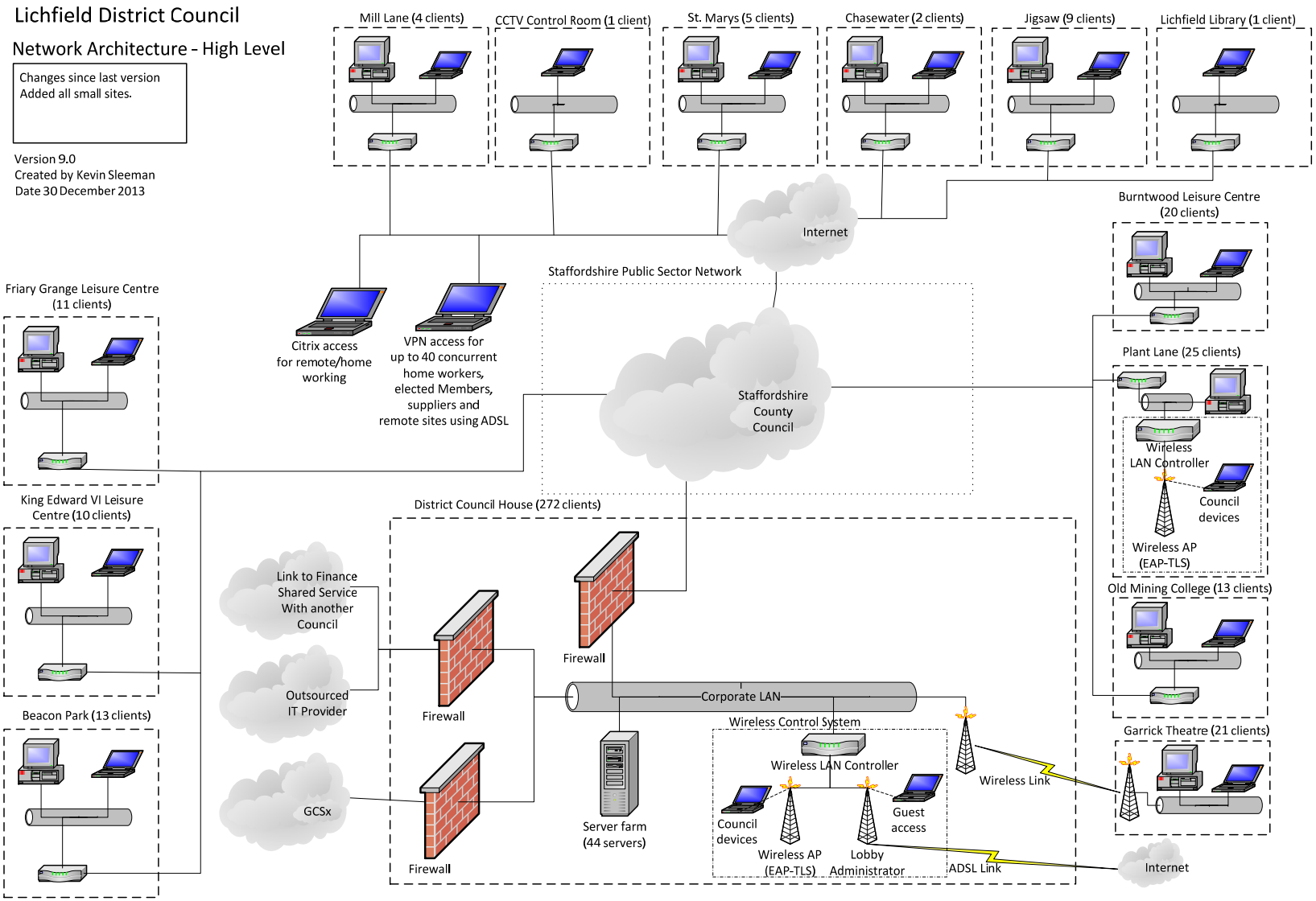
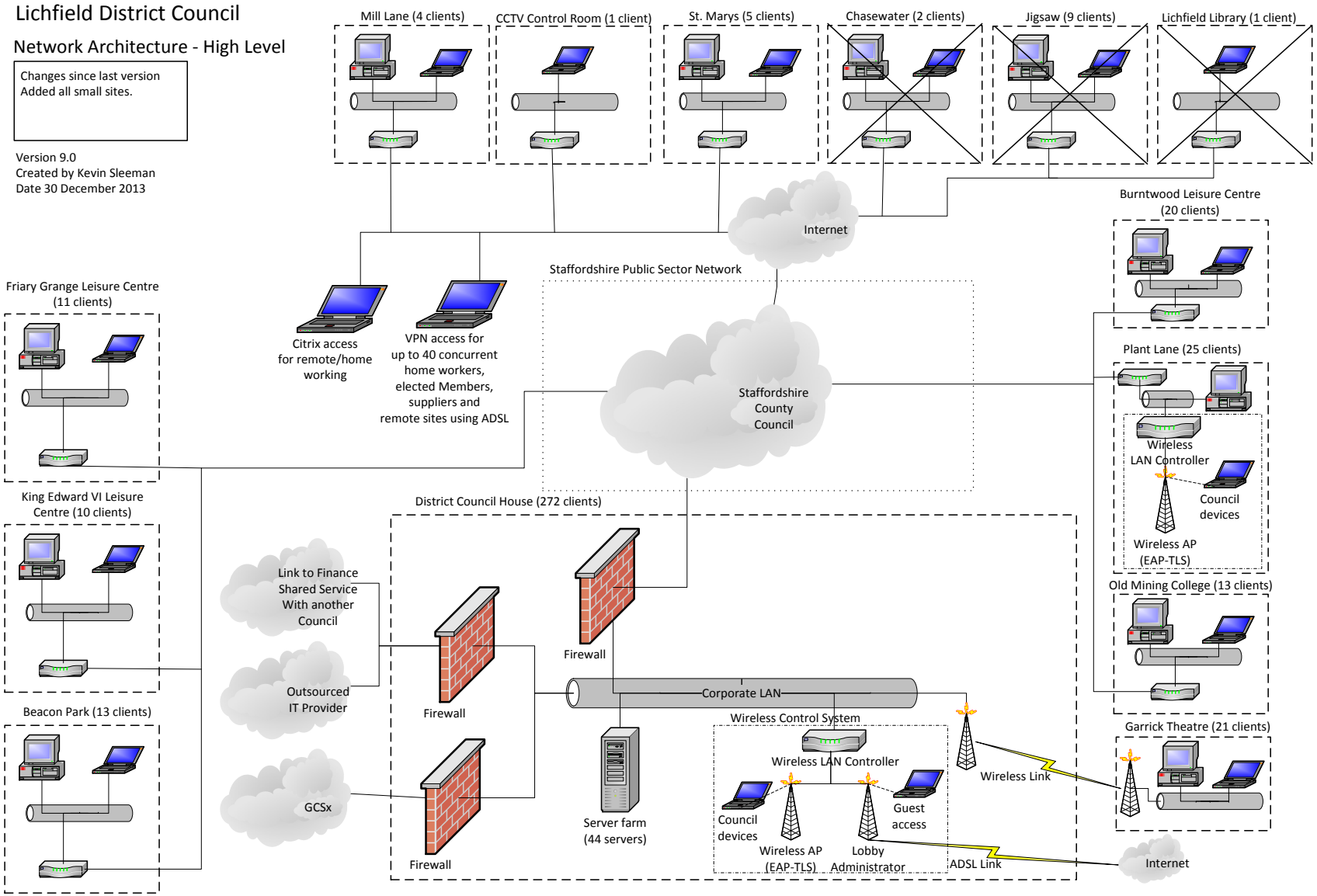
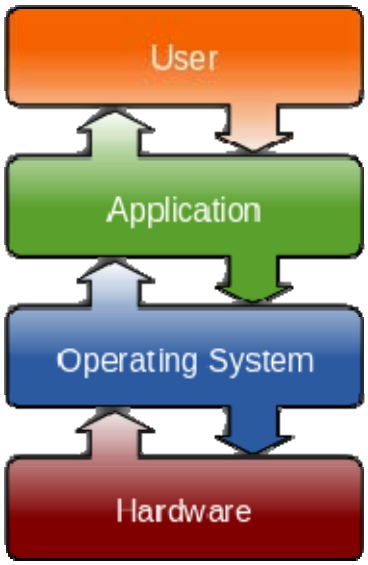


Diagram showing sites where ICT will be located at present when incorporating known future changes.



B.1 The end of support by Microsoft for Windows XP and Office 2003

B.1.1 Released in October 2001, Windows XP has served us well as the tool that runs our computer desktops. As with many technology packages, changes and enhancements are released in the form of new versions. There comes a point where the software company decides that it will no longer spend money on fixing problems with the software; it will encourage people using the software to move forward to newer versions. For Windows XP, Microsoft has decided this date is 8 April 2014. Over the last few years capital funds allocated to the Council's ICT platform have been spent, in part, on upgrading applications used by Revenues and Benefits, Development Control and Building Control, Income Management and the Customer Relationship Management tool used by Lichfield Connects. Upgrading Windows XP is much more significant in terms of change; it is the biggest upgrade possible as every program sits on top of it. The picture below shows how the operating system sits in relation to the other parts of the computer experience.



B.1.2 This is not like the Millennium bug where there was the perception that aircraft would fall from the skies or traffic control systems would stop working; after the 8 April 2014 the computers will still continue to function. The loss of fixes and patches from Microsoft means that over time the Windows XP computers will become more vulnerable to attacks from viruses, keystroke loggers and anything else written to hack into, infect, snoop or steal from them. There will still be anti-virus software available, however that only goes so far. If a problem is found in the Microsoft software, then anti-virus is like wallpapering over a hole in a wall, it masks the issue as long as no-one leans on it.

B.1.3 This situation is not unique to the Council, estimates from the British Computer Society suggest that 85% of PCs in the NHS are still running Windows XP and the NHS employs 1.7 million people. Data collected by a company that monitors internet usage shows that in August 2013 a third of all computers accessing the internet were still running Windows XP.

B.1.4 The challenge of upgrading is the size and complexity of the move and the strategic "onion-peeling" exercise to move to a new platform. The Council's ICT team have a tool that looks at the software installed on the computers and this has found 875 different applications or versions of packages from 298 different suppliers. Each different entry needs to be checked to see if it is compatible with a new operating system or whether a separate upgrade needs to take place.

B1.5 We already know that the company that writes a software application used by the Personnel team have decided to move everyone to their internet based software at a cost of £3,000. The task of evaluating applications compatible with Windows 7 and will be included in the future plans represents one of the largest risks to the project as money is spent testing and converting unnecessary applications. There is further information on the applications and the rationalisation strategy in section B3 of this Appendix.

B.1.6 There is also an issue surrounding historical software applications that needs to be dealt with. This is where software application has changed but the original application is still used to lookup historical information. The software maintenance contract was ended on the original software application when it was changed meaning there is no entitlement on the original software application to an upgrade to support the new operating system. By contacting the original software application developers for advice they may insist on a fresh software maintenance contract and charge for the years of support where the software application has been used outside of support and maintenance.

B.1.7 The risk of not upgrading is that the operating system becomes vulnerable to attack from various bits of software; if an attack exposed customer data the Information Commissioner could impose fines of up to £500,000. The Cabinet Office has also notified the Council that in order to maintain the Public Sector Network link to central government the upgrades will be necessary for the 2014 compliance checks, further detail on this is in Appendix F.

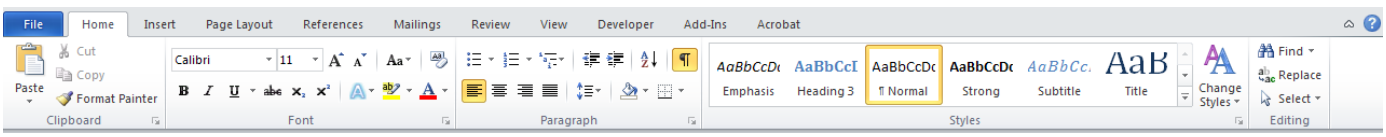
B.2 Microsoft Office 2003

B.2.1 Microsoft Office 2003 was launched in August 2003 and contains a suite of packages used across the organisation including Word, Excel, PowerPoint, Publisher and Access. This package highlights one of the challenges of working in outsourced support environment as Office 2003 was only rolled out across all the desktop and laptop computers in December 2012. Prior to this there had been a mix of Office 2000 and Office XP. The consequence of running different version of the Office package is that the documents we pass around do not like being opened by different versions. Teams such as Internal Business Support Services were finding that their spread-sheets that contained complex formulae and macros were not working.

B.2.2 When Microsoft released the 2007 version of Office they changed some of the underlying code in the programs and as consequence we needed an official Microsoft converter to be able to open files saved in the 2007 format. Since then the 2010 and 2013 version of Office have been released and although the convertor works most of the time it can cause problems and there have been reports of employees having to open files at home on their own computers, that introduces all sorts of risks.

B.2.3 As with Windows XP, Office 2003 has been highlighted in the Cabinet Office communication that says not upgrading will put the Public Sector Network connection to central government at risk. Some copies of Office 2010 have had to be installed for teams such as Finance as they reached the point where they could not complete the financial modelling as the spread-sheet they used was designed using features available in Office 2007 and above and the Office 2003 convertor could not show these features.

B.2.4 One of the main reasons that the Council has stayed with Office 2003 is that it is the last version before Microsoft changed the look of the software and introduced the 'Ribbon interface' shown in the picture below:



B.2.5 In standardising the versions of Office to 2003 there were a number of employees who struggled in moving from Office XP to Office 2003 as the colours of icons had changed. As there is not a corporate ICT training budget it has not been possible to train staff in the newer versions of Office. It has been perceived, backed up by experiences of installing Office 2010 in the Internal Business Support Services team, that there will be a need to train some employees in the new interface, in order for them to remain productive in the short term.

B.3 Application rationalisation

B.3.1 The chart in Appendix C.1 shows that the majority of the laptops and desktops are over eight years old. Over that time software applications used by teams have changed and the old software packages have continued to be used in some cases or not properly uninstalled in other cases. Another software application has been installed on the majority of the computers and this records all of the software that is installed. This software has calculated there are 875 different applications or versions of packages from 298 different suppliers.

B.3.2 By grouping the different versions of applications together and removing those applications run on servers and the premises that are anticipated being transferred to community control then the total number of applications drops to 503. The software application that reports on the software installed also reports on how many times it is used and there are 198 applications that are only installed on one computer and therefore their value to the organisation has to be questioned.

B.3.3 There are already examples that are known of where different applications that serve the same purpose have been installed on different computers. This is particularly relevant with programs to convert documents to a format called PDF. There are eight different applications that achieve this purpose, a purpose that becomes redundant with newer versions of Microsoft Office as it is built into the package.

B.3.4 The application rationalisation strategy will be to work through the list of applications and identify one of the following recommendations for each application:

- Retired from use altogether as it is either redundant or does not deliver the value that a similar application does,
- Modernised so that it supports the later version of Microsoft Windows after a cost assessment of the modernisation has taken place,
- Consolidated and standardise with other applications.

B.3.5 While a critical factor for the success of the project the application rationalisation is a time intensive process and involves the support of the suppliers of the software applications to ensure that they will continue to be supported in the future and that the plans that have been developed do not compromise this situation and to assist in this approach additional resource needs to be brought into the ICT team to provide additional capacity and support.

B.3.6 Once an application has been recommended to be used in the future then further work is needed to ensure that the Council has all of the paperwork in place to prove it is entitled to use the software. Without this in place then there is an inherent risk that the Council may be liable for additional and unscheduled costs in the future.

B.3.7 In an ideal world the application rationalisation would be an iterative process run over a number of months as opposed to attempting to resolve the issues all at once, however in this case time is of the essence regarding the end of Microsoft's support of Windows XP and the Cabinet Office's requirement that Windows XP is removed by September 2014 and therefore it will likely result in an approach where the applications are rationalised in a short space of time.

B.4 Recommendations

B.4.1 When considering a significant change of the operating system it is worth evaluating other options. Although it is the most widely used operating system Microsoft is not the only option. There is the Macintosh operating system produced by Apple along with open source or 'free' options based on the UNIX platform.

B.4.2 The principle issue with moving to other operating systems is that the software applications used by the Officers are not designed to run on other operating systems. While there are software applications such as the Revenues and Benefits tool that only require an internet browser and some support software other applications such as the Planning and Building Control software application have to be installed on top of the operating system. The supplier of this software application only supports Microsoft Windows.

B.4.3 It is therefore recommended that the Council adopts a later version of Microsoft Windows as the new operating system. The choices available are Windows 7 or Windows 8. Windows 7 was released by Microsoft in 2009 and they will support it until 2020. Windows 8 was released in 2012 with the latest version, 8.1, released in October 2013 with support anticipated to end in 2023.

B.4.4 When Microsoft developed Windows 8 they created a new interface for running programs that was designed for desktop computers, laptops, tablet computers and smartphones. This new interface was initially criticised for being difficult to learn, particularly when used with a keyboard and most as opposed to the touchscreen it had been designed for. Window 8.1 has addressed this criticism however the companies that produce the software applications the Council uses have yet to test the system and make it part of their supported systems. It is for this reason that it is recommended that the replacement operating system is Windows 7. The Council already has a contract with Microsoft for the supply of the operating system and the costs of the software will be met from that existing annual payment.

B.4.5 As with the operating system alternative applications to Microsoft Office are available to enable the creation of documents and spreadsheets. As with the operating system alternatives it is the companies who write the Council's main business software applications that only test their products with Microsoft Office. In the case of the Planning and Building Control system the software supplier does not prevent the Council from looking at other applications, however they will not provide any support if the links from their software application does not work. In addition they would expect the Council to take on the responsibility of writing the programs that make their software application work with the alternative package. If there are any faults discovered they will only look at them if the same fault can be replicated when using a copy of Microsoft Office.

B.4.6 Any impacts on the contract with the outsourced IT support provider also needs to be considered when looking at an alternative to Microsoft Office. When the contract was being put in place all of the potential suppliers said they could support alternative software applications to Microsoft Office, however, each supplier said they would expect the Council to bear any costs for training their staff in the different application so they could support it.

B.4.7 For these reasons it is recommended that the Council continues to use Microsoft Office for the creation of documents and spreadsheets. There are three versions of Microsoft Office available, 2007, 2010 and 2013. There will be a need to provide training for Members and Officers in the new desktop system and it would therefore be most cost effective to adopt the 2013 version of Office. Although this is not supported by the companies that write the software applications, the risk of finding issues is judged less than with the operating system as the changes between the commonly supported Office 2010 and Office 2013 were less than in the case of the operating system. The Council already has a contract with Microsoft for the supply of Microsoft Office and the costs of the software will be met from that existing annual payment.

B.4.8 The agreement with Microsoft also includes additional licences for a product called Lync. This software ties together Microsoft Office with the new intranet tool, SharePoint, currently being developed and is linked to the telephone system provided by Staffordshire County Council and the email system to allow people to collaborate on creating documents, to more effectively worked with people from other organisations who also use the tool and for the Lichfield Connects staff to have greater visibility on when employees are in the office and provide a best service to the customer.

B.4.9 With the assistance of the Council's Training and Development Officer the cost of providing appropriate levels of conversion training has been developed. These costs would give all Members and Officers an overview of the new versions along with the Government Security Classification scheme the Council is required to implement. In addition 150 people who use more advanced Word and Excel features would receive two half days of additional training.

B.4.10 In addition to training, the agreement with Microsoft gives the ability for copies of Microsoft Office 2013 to be purchased by Members and Officers for around £9 to install on their home computers. Online training is also included and a previous Microsoft account manager has suggested that they may assist with a day of events to assist in helping people to adapt to the changes.

B.4.11 Application rationalisation will take a considerable amount of time to work through the list of applications and make a decision regarding the future of each application. There are specialists in the market that could assist and undertake this work, however, the daily rate is approximately £2,000-£3,000 per day. The Council's ICT Team will need to manage the process as the specialists will understand the software applications, but not the context of the business. The Council's ICT team consists of three full time employees who in addition to managing the Council's ICT contract and the delivery of the Council's technology plan are also responsible for procurement for the Council. Therefore, it is recommended to increase the capacity of the Council's ICT Team by temporary employment of an additional resource for a period of up to 18 months. The purpose of this resource will be to focus on the upgrade providing project and to assist with project management, testing of applications and arranging training.

B.4.12 As part of the application rationalisation there will be a need to cease use of some of the older systems. The Council has statutory requirements to hold financial and payroll information for anything between seven and 13 years. Where software applications have been either upgraded or moved to new systems the original information has been kept in its original format. As a consequence the Council is operating a number of old servers with expensive licences to provide access to this historical information if needed. Some work has been completed to identify a new software application for this information and a tool has been identified for this purpose. The purchase of this new tool and cessation of the old applications will reduce the Council's annual software licence costs by around £25,000 per year.

B.4.13 As the number of Council Officers is reduced there is a need for these Officers to have a wider ranging set of skills. This project gives the opportunity to assist the Council in ensuring that the Officers are aware of changes to the Council's policies and procedures. With new software, policies and procedures that change can be displayed on an Officer's screen and then a short test can be undertaken. If an Officer fails to meet the pass mark this is flagged to the Training and Development Officer who can arrange further training on that policy or procedure. This supplements the Council's training records and will become an essential tool in demonstrating that the Council has trained Officers in the various policies and procedures it has.

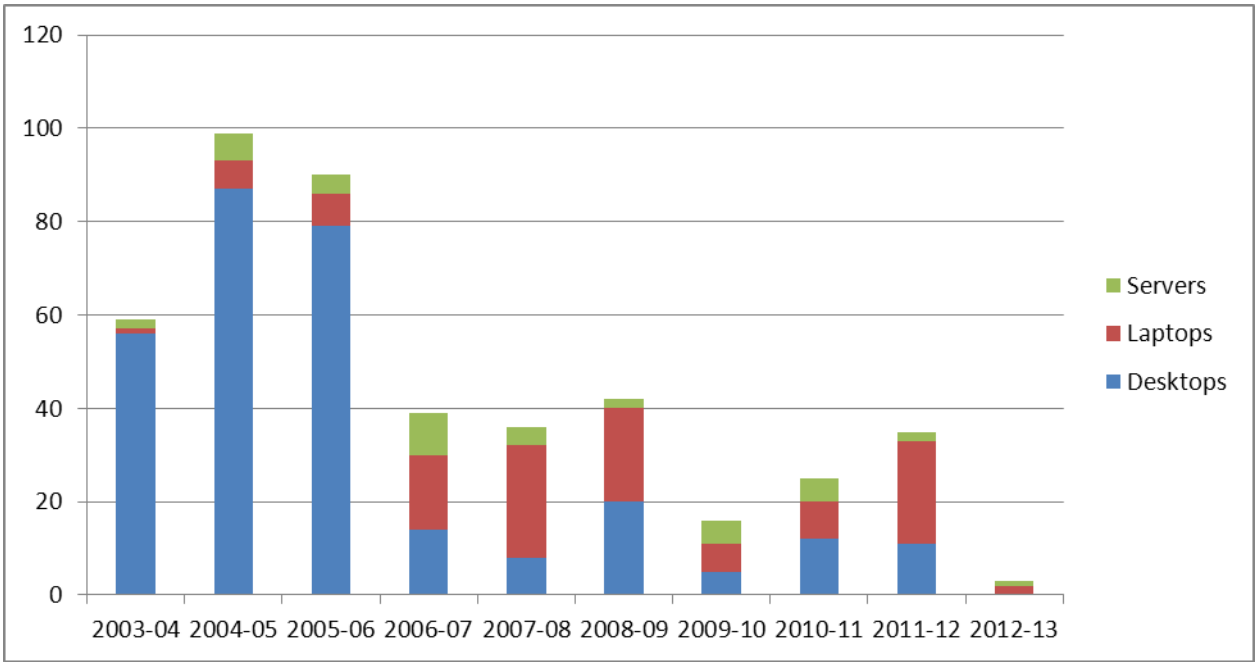
B.5 Costs

B.5.1 The cost below shows the five year expenditure for the recommendations described in this Appendix.

Type of Expenditure	Year 1		Year 2		Year 3		Year 4		Year 5		Total	
	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue
	£	£	£	£	£	£	£	£	£	£	£	£
Investments												
Project Management	24,220	0	12,110	0	0	0	0	0	0	0	36,330	0
IT Licenses/Agreements	0	5,000	0	5,100	0	5,200	0	5,310	0	5,410	0	26,020
Training	20,000	0	0	0	0	0	0	0	0	0	20,000	0
ICT Contract	0	1,600	0	1,630	0	1,660	0	1,690	0	1,730	0	8,310
Software	18,280	470	0	480	0	490	0	500	0	510	18,280	2,450
Professional Fees	15,000	0	0	0	0	0	0	0	0	0	15,000	0
Total	**£77,500**	**£7,070**	**£12,110**	**£7,210**	**£0**	**£7,350**	**£0**	**£7,500**	**£0**	**£7,650**	**£89,610**	**£36,780**
Total plus 2% contingency	**£79,370**	**£7,240**	**£12,400**	**£7,380**	**£0**	**£7,530**	**£0**	**£7,680**	**£0**	**£7,830**	**£91,770**	**£37,660**
Savings												
IT Licenses/Agreements	0	(35,220)	0	(35,220)	0	(35,220)	0	(35,220)	0	(35,220)	0	(176,100)
ICT Contract	0	(4,770)	0	(4,770)	0	(4,770)	0	(4,770)	0	(4,770)	0	(23,850)
Total	**£0**	**(£39,990)**	**£0**	**(£39,990)**	**£0**	**(£39,990)**	**£0**	**(£39,990)**	**£0**	**(£39,990)**	**£0**	**(£199,950)**
Grand Total	**£79,370**	**(£32,750)**	**£12,400**	**(£32,610)**	**£0**	**(£32,460)**	**£0**	**(£32,310)**	**£0**	**(£32,160)**	**£91,770**	**(£162,290)**

C.1 Servers and desktop that have passed their useful life

C.1.1 Many of the servers that hold the software applications used every day along with the desktop computers have passed the end of their useful life. As more and more is demanded from them they become slower and slower. Simply replacing them with new machines is not always an option. In a bid to encourage people from using Windows XP to using a newer version Microsoft stopped the hardware companies from producing Windows XP versions of the software that make the components in the computers function properly. The chart below shows when the servers, desktops and laptops were purchased and the number purchased in that year.



C.1.2 In order to add Windows 7 or Windows 8 computers to the network there is preparatory work required by the ICT support provider to ensure that where possible the best practice guidance from the Cabinet Office on the required settings is followed.

C.1.3 A comparison of Microsoft's recommended specification for Windows 7 compared to the current estate shows that of the 390 devices only 94 meet this specification with 294 needing more memory. In addition there were machines that did not have a powerful enough processor or a large enough hard drive. There was not enough information available to check that the hardware that displays the pictures on a screen met the specification, meaning that there could be more computers that do not meet the specification.

C.1.3 In order to support the features of recent versions of Microsoft Office the core programs such as email need to be upgraded. These core programs put increased demands on the server hardware have changed and the older servers currently in use will be unable to support them and as a consequence need replacing.

C.1.4 The Council is already starting to experience the effects of running the older servers. The Customer Relationship Management System purchased through Staffordshire Connects cannot be fully implemented as this requires features that are only available in a newer version of the program that runs the email system.

C.2 Recommendations and costs

C.2.1 The recommendations and costs are contained in Appendix H.

D.1 Fitness of the current server room

D.1.1 The room that the servers sit in has been adapted over many years and it is no longer able to support a modern operating environment. There needs to be strengthening of the walls to bring it up to the latest reasonable standards of fire protection and to ensure the air conditioning and battery protection units are fit for purpose.

D.1.2 New battery protection units have recently been purchased at a cost of £4,800. These units are a cost effective and short term fix to provide battery back-up in the event of mains failure as they are not designed to work with the generator. They are designed to work with a mains power supply that provides a constant voltage whereas the voltage produced by the generator varies more significantly. The cost of putting in the correct type of battery protection unit is estimated at five times the cost of the ones recently purchased.

D.1.3 The walls of the server room would only provide protection for a maximum of 15 minutes, the ICT industry recommendation is for a maximum of one hour.

D.1.4 There is protection in the event of a major power failure as the generator would start providing power after about 15 seconds; however the life of the current battery protection units will be shortened by the generator running and if the battery protection units cannot provide the 15 seconds of cover the servers will crash. When the server crashes it may cause data to be lost or corrupted. The servers need to be brought back in up in a particular order otherwise they do not start properly and this process can take up to an hour, during that time the business would be unable to work.

D.1.5 There is a gas system to protect the server room if there is a fire in the server room and this is tested annually to ensure it provides at least the recommended ten minutes of protection, however if the fire starts in the corridor outside the server room then the walls would last a maximum of 15 minutes before they were burnt and the gas suppression system would be become ineffective. We have to rely on the fire service having the fire under control within 15 minutes of it starting.

D.1.6 The risk from the two air conditioning units is that they have reached the end of their design life and are working at capacity even when the external temperature is below zero. When one unit fails, the second tries to cool the whole of the room and as a consequence tends to freeze up and fail. Without any air conditioning the temperature in the room raises and within an hour the servers will start to shut down in order to protect their components.

D.2 Recommendations and costs

D.2.1 The recommendations and costs are contained in Appendix H.

E.1 Business continuity

E.1.1 The challenge relating to business continuity is the ability of the Council to continue working if the server room is destroyed.

E.2 Current arrangement if the server room is destroyed

E.2.1 Currently, the Council's data is backed up to tapes, using a tape drive that is no longer supported by the manufacturer and the tapes are taken to another building owned by the council for storage in a fire proof safe. The volume of data the Council now has also exceeds the maximum capacity for the tapes that can be held in the tape unit at any one time and as a consequence the weekend backups can run over into working time on a Monday.

E.2.2 The tapes are transferred using a secure cash courier service however if the tapes were stolen from the courier then potentially someone with the right sort of equipment could get to the Council's customer data and then the Council would be at risk of prosecution from the Information Commissioner.

E.2.3 The current business continuity arrangements offer a number of options. In the event of a piece of equipment failing then there is a support and maintenance contract with a third party company who will attempt to fix the problem within about one working day. If they are unable to fix the equipment and it is a piece of equipment on the business continuity contract with the ICT support provider then they would have three working days to deliver the kit to an alternative Council premises where the data could be put restored and the service brought back online.

E.2.4 There is testing of the business continuity to ensure that the data can be restored and the Revenues and Benefits application was tested in 2012 with Planning and Building Control scheduled for 2014.

E.2.5 The principle risk of not upgrading is the question of whether three working days for equipment to be delivered is an acceptable delay or whether there must be equipment ready to take over at any moment. It would be prohibitively expensive to have every system fully connected to two separate server rooms but there are things that can be done to ensure that some of the systems can be moved over within hours rather than days.

E.2.6 The other risk is that the business continuity solution has never been fully tested. There has never been a truck of the appropriate size turn up at the alternate premises to ensure it can fit through gates or connect into the network to provide the services.

E.3 Recommendations and costs

E.3.1 The recommendations and costs for resolving the issue are contained in Appendix H.

F.1 The threat of disconnection from Central Government networks by the Cabinet Office

F.1.1 Since the loss of computer disks containing 25 million child benefit recipients by HMRC in 2007, Central Government departments have been tightening up on the need to protect the public's personal information. Gone are the days of sending cds in the post and hoping they turn up at the desk of the person they were intended for.

F.1.2 The Council has had a direct IT network connection to Central Government since 2009 and it is currently used in the following ways:

- The Revenues and Benefits team receive daily updates from the Job Centre Plus on changes of the details on people who register for their services,
- Revenues and Benefits team members can connect to a DWP system to check on the benefits people may be getting from other organisations and government departments,
- Lichfield Connects receives information from the Tell-Us-Once service that is run by the Bereavement Services at the Registry Offices so that the family of the person do not need to contact lots of different agencies,

- Registering to vote is changing from a single declaration per household to everyone having to register individually and the Electoral Commission will be compiling the countrywide register using the network,
- There are 40 employees with secure email accounts to allow secure exchange of emails, the latest being Environmental Health to receive food related notices from the Health Service.

F.1.3 The Cabinet Office assumed responsibility for the process of ensuring that each local authority is managing its IT security to the prescribed standard in April 2013. They have introduced a significant number of changes that makes meeting the security standards much more difficult.

F.1.4 The implication of not meeting the security standard is that the connection to Central Government would be switched off and the ability to gain access to those services above would cease. Revenues and Benefits in particular would no longer be able to deliver their statutory services.

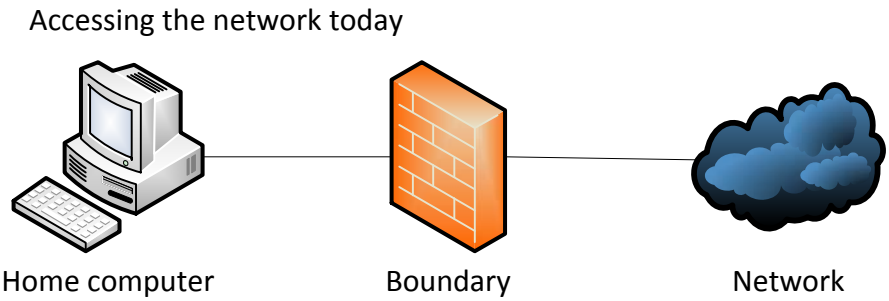
F.1.5 In order to mitigate the risk the ICT team are working to address the current set of concerns that the Cabinet Office has with our submission. Each year we have to employ an external company that provides a "hacking" service to attack the IT network from both the inside and outside. When they have completed their attacks we have to fix all of the high and medium rated risks they identify before the Cabinet Office will accept our submission. This year there were ten high rated risks and 19 medium rated risks. This is one example of where the rules have been tightened. In previous years work to fix these risks would have been carried out at the same time as going through the accreditation process. This year, however, all risks rated as high or medium must be addressed before a submission is made.

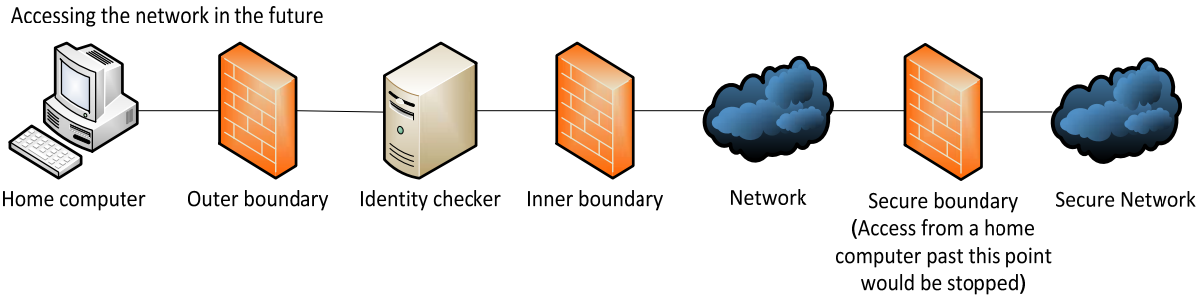
F.1.6 Although there are specific issues with accessing systems from personal computers and the Council's laptops and memory sticks below there is a need to replace the current logging tool. The requirements for the connection expect that all access of systems will be logged and these records kept for six months. The current system is not fit for purpose and an alternative product from Trustwave has been identified as appropriate for the needs and size of the Council.

F.1.7 In addition the wireless units that provide Members with access to the internet and Officers access to their documents are reaching the end of their lives and need to be replaced in order to remain compliant with changing standards.

F.2 Access from personal computers

F.2.1 The diagrams below attempt to illustrate the situation the ICT team are dealing with when looking at home working and the gap between the current position and how the network needs to be secured.





F.2.2 When information provided by central government services is held in our applications the security of each application has to change. Each of these applications cannot be allowed to be accessed from an employee's home computer. This is because the security of the home computer cannot be as robustly assessed in the same way that a computer owned by the Council can be. It was announced in August 2013 that a Council had been fined £100,000 by the Information Commissioner as a home computer used by a social worker had a program installed that transferred sensitive information about several vulnerable children and their families to a publicly accessible website.

F.2.3 The software applications that currently hold Central Government information are:

- Council Tax and Benefits administration
- The Council's document management system used by Revenues and Benefits, Planning and Building Control, Cashiers and Environmental Health
- Management of the electoral register
- Customer Relationship Management used by Lichfield Connects and other teams across the Council, this may be included but further work is needed to understand where the Tell-Us-Once information is recorded.

F.2.4 In the short term a Council can allow access to those systems that do not hold any Central Government information. It would appear that in the longer term, as more government systems come onto the network more applications will be included in the restricted list. Rather than removing all home working access the affected applications listed above have been removed from the home working application Citrix. The Citrix products are powerful and work is being undertaken to understand if they can tell the difference between a Council and personal owned computer.

F.2.5 In the long term there is a need to introduce some new servers to ensure that the Blackberry and Good services are properly segregated and a technology called two-factor authentication. Currently only a username and password is required to access external facilities such as Outlook Web Access, however, there is a need to have an additional verification method such as a code that changes every time it is used. An example of two-factor authentication in everyday use is accessing a bank account through an automated teller machine (ATM). In order to withdraw money there is a need to have both the bank card (something physical) and the personal identification number (PIN) code (something that is known). In order to add an extra level of security there is a need to also have two different usernames and passwords to get access to the network, knowing the outer username and password will only give access to the identity checking services.

F.2.6 This will have an impact on Members and Officers as it will lead to the closing of Outlook Web Access and a migration over to Citrix. The reason is that Outlook Web Access allows email attachments to be saved to a computer outside of the control of the Council and this breaches the guidance from the Cabinet Office. In addition an additional Microsoft Exchange server would need to be implemented. The licence for Microsoft Exchange costs £310 and there would be £1,590 of additional annual costs from the outsourced IT provider to maintain the server. Further details on changes proposed for Member's ICT access is contained in Appendix H.

F.2.7 In order to comply with the secure email requirements there is a need to either implement an additional Microsoft Exchange server or to buy a secure email service from another company. Vodafone, the provider of the connection to the Central Government network, offer such as a service costing £3.66 per mailbox per month. The Council has 40 secure mailboxes that would be an annual cost of £1,760. Although the costs are virtually the same as operating an internal server, moving the mailboxes to a Vodafone provided solution will enable the costs to be directly allocated to the team that are using them and mailboxes can be added or removed as required with them being charged on a monthly basis.

F.3 Encrypted memory sticks and hard drives

F.3.1 Memory sticks and laptops are called portable devices as they can be easily moved around. If they can be easily moved around, they are at risk of being stolen or left somewhere such as a train or taxi. It is not possible to stop the use of portable devices as they so underpin the way that IT works, so the requirement from the Cabinet Office is that they are encrypted. Encryption is a technique where the portable device cannot be used unless the correct password is given or an extra security tag is plugged into it.

F.3.2 The ICT Team has purchased enough licences for 70 laptops and although there are around 100 laptops in the Council an assessment is required of those that do not leave the building and are used as desktop computers. In the case of these machines they will need to be locked to the desktop to prevent them being stolen. There has been a case recently of the Information Commissioner imposing a penalty on an authority for having an unencrypted laptop stolen from the office and we need to be mindful of this in making decisions.

F.3.3 The anti-virus software the Council uses has been recording the use of memory sticks and determined that over a 16 week period between April and September 2013 memory sticks were used in 161 computers, some 33 were accessed once. Having worked with the Government Procurement Service reseller a model of memory stick has been identified that complies with the security requirements and also has the ability to be managed centrally so that if the encryption password is forgotten it can be reset without having to throw the memory stick. The costs of 100 memory sticks has been included in the costs below, however further work is required to identify exactly who is using a memory stick and needs a new stick. The costs that have been included are for a 4GB memory stick and by adopting a catalogue approach the costs of purchasing larger capacity memory sticks will be available.

F.4 Mobile devices

F.4.1 Where the Council owns and is using smartphones and tablets such as iPads there is a requirement for the connection to be secured using an Access Point Name (APN). This ensures that the data from the smartphone or tablet is sent securely to the Council systems. The ICT team are already working on implementing a new mobile phone contract that will replace the existing handsets however the APN is a new requirement that is needed to prevent the devices becoming non-compliant with the latest Cabinet Office guidance.

F.5 Identity checking

F.5.1 The Cabinet Office have include the requirement initially for everyone accessing PSN services or PSN originated data will need to meet the Baseline Personnel Security Standard and by 2015 everyone with access to the Council network will need to have been accessed.

F.5.2 The Baseline Personnel Security Standard involves four main elements:

- Identity Check
- Nationality and Immigration Status
- Employment history (past three years)
- Verification of Criminal Record (unspent convictions only)

F.5.3 The Cabinet Office has issued guidance relating to this process that the Verification of Criminal Record must be independent and not a self-declaration. Although there is no requirement for a full Disclosure and Barring Service check where a member of staff already been subjected to a check they do not need a Verification of Criminal Record check as well. The requirement is for verification of unspent convictions only. In order to undertake this then there is a cost of £25 per application from a service such as Disclosure Scotland. The costs of a one-off check for 400 Members and Officers have been included in the cost table below. As this is a pre-employment check then the ongoing cost will have to be paid by the team making the recruitment.

F.6 Recommendations

F.6.1 The core logging solution needs to be replaced as it is not fit for purpose and it is recommended that it is replaced with a solution from Trustwave and the wireless units that are approaching the end of their lives are replaced with new units.

F.6.2 New servers needs to be implemented to allow Blackberry and Good services to remain compliant with the Cabinet Office design guidelines and the existing investment in two-factor authentication is upgraded to comply with the requirements.

F.6.3 In order to assist with the requirements it is recommended that there is a transition from Outlook Web Access to Citrix with the closure of Outlook Web Access and the secure email boxes are moved to the solution provided by Vodafone.

F.6.4 It is recommended that encrypted memory sticks are purchased and that laptops that are not taken from the office are secured to desks.

F.6.5 In order to ensure that Council owned mobile phones and tablets remain compliant that the Access Point Name is purchased.

F.6.6 To ensure that the identity checks are completed with the Cabinet Office requirements it is recommended that a programme of checking is commenced with those staff that have not been CRB checked undertaking a Verification of Criminal Records check.

F.7 Costs

F.7.1 The cost below shows the five year expenditure for the recommendations described in this Appendix:

Type of Expenditure	Year 1		Year 2		Year 3		Year 4		Year 5		Total	
	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue
	£	£	£	£	£	£	£	£	£	£	£	£
Investments												
Staffing	10,000	0	0	0	0	0	0	0	0	0	10,000	0
IT Licenses/Agreements	0	3,740	0	3,820	0	3,890	0	7,410	0	7,560	0	26,420
ICT Contract	0	3,200	0	3,250	0	3,320	0	3,390	0	3,450	0	16,610
Hardware	42,540	0	0	0	0	0	0	9,000	0	9,180	42,540	18,180
Professional Fees	13,450	0	0	0	0	0	0	0	0	0	13,450	0
Total	**£65,990**	**£6,940**	**£0**	**£7,070**	**£0**	**£7,210**	**£0**	**£19,800**	**£0**	**£20,190**	**£65,990**	**£61,210**
Total plus 2% contingency	**£67,580**	**£7,110**	**£0**	**£7,240**	**£0**	**£7,380**	**£0**	**£20,280**	**£0**	**£20,680**	**£67,580**	**£62,690**
Savings												
Broadband	0	(1,500)	0	(1,500)	0	(1,500)	0	(1,500)	0	(1,500)	0	(7,500)
IT Licenses/Agreements	0	(910)	0	(910)	0	(910)	0	(910)	0	(910)	0	(4,550)
Total	**£0**	**(£2,410)**	**£0**	**(£2,410)**	**£0**	**(£2,410)**	**£0**	**(£2,410)**	**£0**	**(£2,410)**	**£0**	**(£12,050)**
Grand Total	**£67,580**	**£4,700**	**£0**	**£4,830**	**£0**	**£4,970**	**£0**	**£17,870**	**£0**	**£18,270**	**£67,580**	**£50,640**

G.1 Review of the ICT Access, Use and Security Policy

G.1.1 The Council has had a number of different sets of IT procedures over the last few years with the latest set being written in 2009 in response to the introduction of the Government's secure network. They were written as part of a government sponsored project involving every West Midlands authority. These procedures were approved by the Employee Liaison Group and were communicated to managers through a session at Breakfast Brief. Recently there have been some changes and some concerns that led to the procedures being revised. These have included:

- The current procedures were written prior to tools such as Facebook and Twitter and do not offer the Council sufficient protection to take action against employees posting derogatory comments about the Council in their own time on their own computers.
- The establishment of the Garrick Theatre Trust led them to needing their own set of procedures so they can demonstrate to the Charity Commission that they are independent from the Council,
- Changes to the Cabinet Office rules for remaining connected to the Public Sector Network and the proposed introduction of document classification,
- Members and employees were signing the section relating to Internet and email as opposed to the whole document,

G.1.2 The most significant change is the length of the document. The 2009 version comprised of 17 separate documents that was actually one document less than the version it replaced. It comprised of almost 180 pages using a lot of language better suited to large authorities. The new version of the procedures is a single document that is shorter and uses a more 'plain English' style of language and is attached in Appendix K. Due to the length of the policies it has been placed as the last Appendix of this report.

G.1.3 The procedures have gained a dedicated section on social media but chapters on legal responsibilities and the recruitment process have either been removed or stripped back with references to the appropriate section responsible for that area.

G.1.4 There are no references to the Council in the procedures and this is done deliberately so that they can be used by the Garrick Theatre. The intention is that the two documents remain broadly the same as differences between them increases the risk that the ICT support provider can introduce charges for managing different sets of procedures.

G.1.5 A new personal commitment statement has been added. This commitment statement has been developed by the Councils using the Staffordshire Connects Customer Relationship Management system. It is a requirement of accessing their system that every employee signs the personal commitment statement, by including the statement in the procedures the intention is to reduce the amount of forms that need to be signed.

G.2 Recommendations

G.2.1 It is recommended that the policy in Appendix K is adopted by the Council.

G.2.2 A two stage sign off approach is recommended for their adoption by all Members and Officers. In tandem with other sections of the document and by working through the Council Officers will be asked to sign a document saying they have been told where on the intranet to get the policy. For subsequent new starters this will be a copy of the policy. After 28 days they will be asked to sign to say they have read and understood them. This gives the Member or Officer the opportunity to ask any questions about the policy or discuss general IT issues.

G.3 Costs

G.3.1 There are no costs associated with this Appendix as the administration resource has been covered in other parts of the document.

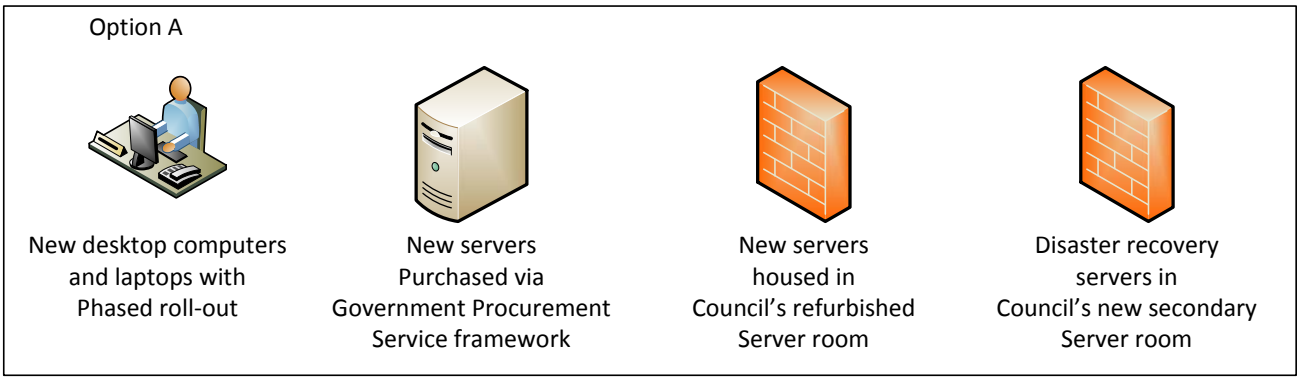
H.1 Options that have been considered

H.1.1 The ICT industry is awash with terms such as ‘cloud computing’ or ‘virtualisation’ and there is no real definition as to what these terms mean as they are different to each organisation depending on their unique set of operating conditions.

H.1.2 The ICT Review Group took a more pragmatic approach and considered the two factors of who owns the equipment and where is the equipment stored. This led to the development of the matrix below allowing all of the options considered to be slotted.

Option	Equipment located in Council server room	Equipment located in third party server room
Council owns the equipment	Options A and B	Option C
Third party owns the equipment		Option D

H.1.3 The ICT Review Group then considered each of the options in greater depth to appreciate the implications for the Council of each proposal.

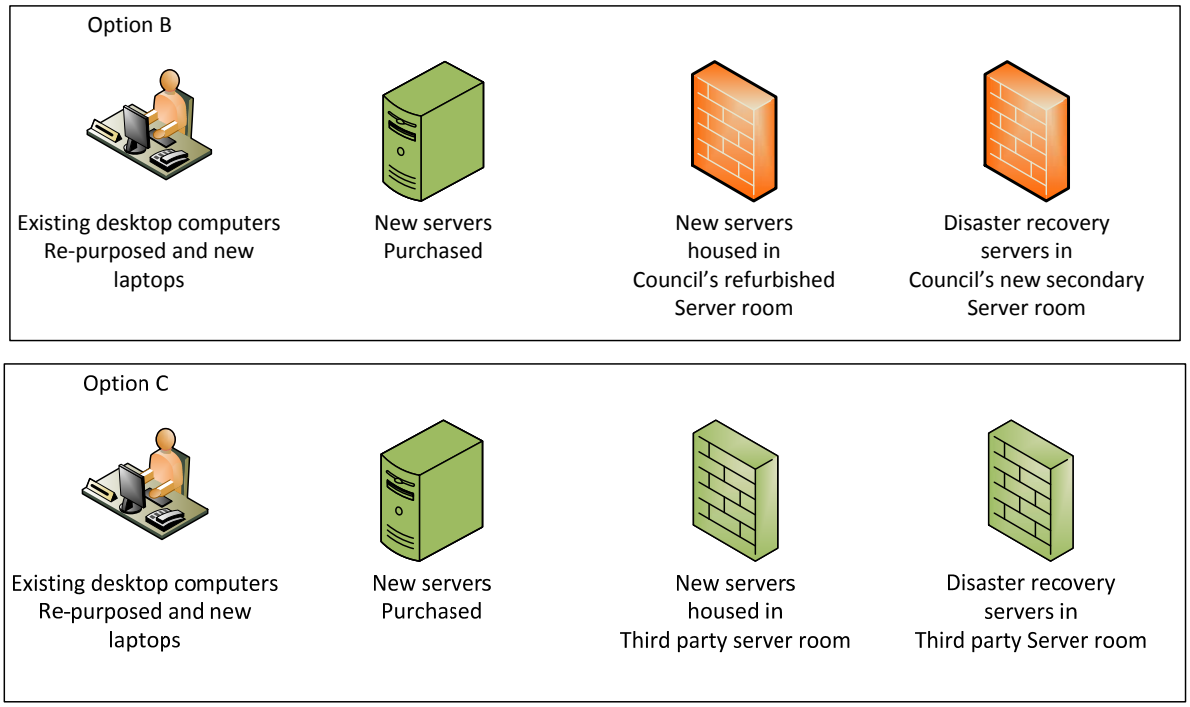


H.1.4 Option A. This option mirrors a traditional replacement programme. This works by replacing existing equipment with new equipment essentially making tactical upgrades as opposed to strategic change that puts the Council in the best position for the future. This option includes not only upgrading the existing server room to make it fit for purpose, but also creating a secondary backup server room at an alternative premise. There are already facilities at this location, but there would need to be increased security and new fire suppression systems. The advantages and disadvantages of this option are:

- Advantages
  - Re-instates traditional replacement programme
  - Allows for a staged roll out of new equipment
- Disadvantages
  - There is limited space to expand
  - The Proposed business continuity location would need retro-fitting
  - The costs of running two server rooms remain with the Council
  - It will cause extended period of disruption as everyone is brought onto the new platform
  - There may not be sufficient time to comply with Cabinet Office requirements
  - Business continuity would be enhanced but only for those services deemed as critical.

H.1.5 The costs of option A are shown below:

Type of Expenditure	Year 1		Year 2		Year 3		Year 4		Year 5		Total	
	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue
	£	£	£	£	£	£	£	£	£	£	£	£
Investments												
Broadband	5,000	5,430	0	5,540	0	5,650	0	5,770	0	5,880	5,000	28,270
IT Licenses / Agreements	0	22,250	0	26,620	0	27,150	0	27,700	0	28,250	0	131,970
ICT Contract	0	15,890	0	16,160	0	16,480	0	16,810	0	17,150	0	82,490
Hardware	620,320	0	43,300	0	32,900	0	64,600	0	124,100	0	885,220	0
Software	113,150	0	1,920	0	0	0	0	0	0	0	115,070	0
Professional Fees	426,150	0	0	0	0	0	0	0	0	0	426,150	0
Total	**£1,164,620**	**£43,570**	**£45,220**	**£48,320**	**£32,900**	**£49,280**	**£64,600**	**£50,280**	**£124,100**	**£51,280**	**£1,431,440**	**£242,730**
Total plus 2% contingency	**£1,192,690**	**£44,620**	**£46,310**	**£49,480**	**£33,690**	**£50,470**	**£66,160**	**£51,490**	**£127,090**	**£52,520**	**£1,465,940**	**£248,580**
Savings												
IT Licenses / Agreements	0	(3,380)	0	(3,380)	0	(3,380)	0	(3,380)	0	(3,380)	0	(16,900)
ICT Contract	0	(11,000)	0	(11,000)	0	(11,000)	0	(11,000)	0	(11,000)	0	(55,000)
Total	**£0**	**(£14,380)**	**£0**	**(£14,380)**	**£0**	**(£14,380)**	**£0**	**(£14,380)**	**£0**	**(£14,380)**	**£0**	**(£71,900)**
Grand Total	**£1,192,690**	**£30,240**	**£46,310**	**£35,100**	**£33,690**	**£36,090**	**£66,160**	**£37,110**	**£127,090**	**£38,140**	**£1,465,940**	**£176,680**



H.1.6 Options B and C. Options B and C utilise the same technology, however for option B the equipment is located in the Council's server room whereas option C uses another organisation's server room. Options B and C also have two variations. Variation B1 and C1 uses equipment sourced through the ICT support provider whereas variation B2 and C2 uses a Staffordshire County Council framework to procure the equipment.

H.1.7 The advantages and disadvantages of option B are:

- Advantages
  - Reduced dependence on ICT provider at end of ICT support provider contract
  - There are less organisations involved making it less complex to support
- Disadvantages
  - Limited space to expand
  - Proposed business continuity location would need retro-fitting
  - The costs of running two server rooms remain with us

H.1.8 The advantages and disadvantages of option C are:

- Advantages:
  - Reduced cost overall for the Council
  - Uses robust server rooms designed for purpose
  - Business continuity designed from the start
  - Gives ability to support future strategy
- Disadvantages:
  - Exit arrangements at the end of ICT support contract need to be considered
  - Infrastructure more complicated as more companies are involved
  - Dedicated data links are required to the ICT support provider data centre
  - The historical servers need to be retired

H.1.9 The costs of Option B1 are:

Type of Expenditure	Year 1		Year 2		Year 3		Year 4		Year 5		Total	
	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue
	£	£	£	£	£	£	£	£	£	£	£	£
Investments												
Broadband	5,000	5,430	0	5,540	0	5,650	0	5,770	0	5,880	5,000	28,270
IT Licenses / Agreements	0	7,950	0	8,110	0	8,270	0	8,440	0	8,610	0	41,380
Hardware	132,940	0	4,500	0	3,500	0	24,100	0	12,500	0	177,540	0
Software	73,580	0	0	0	0	0	0	0	0	0	73,580	0
Professional Fees	1,057,100	80,300	0	81,650	0	83,280	0	84,950	0	86,640	1,057,100	416,820
Total	**£1,268,620**	**£93,680**	**£4,500**	**£95,300**	**£3,500**	**£97,200**	**£24,100**	**£99,160**	**£12,500**	**£101,130**	**£1,313,220**	**£486,470**
Total plus 2% contingency	**£1,299,190**	**£95,940**	**£4,610**	**£97,600**	**£3,580**	**£99,540**	**£24,680**	**£101,550**	**£12,800**	**£103,570**	**£1,344,860**	**£498,200**
Savings												
Security	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(13,000)
IT Licenses / Agreements	0	(5,980)	0	(5,980)	0	(5,980)	0	(5,980)	0	(5,980)	0	(29,900)
ICT Contract	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(180,000)
Total	**£0**	**(£44,580)**	**£0**	**(£44,580)**	**£0**	**(£44,580)**	**£0**	**(£44,580)**	**£0**	**(£44,580)**	**£0**	**(£222,900)**
Grand Total	**£1,299,190**	**£51,360**	**£4,610**	**£53,020**	**£3,580**	**£54,960**	**£24,680**	**£56,970**	**£12,800**	**£58,990**	**£1,344,860**	**£275,300**

H.1.10 The costs of Option B2 are:

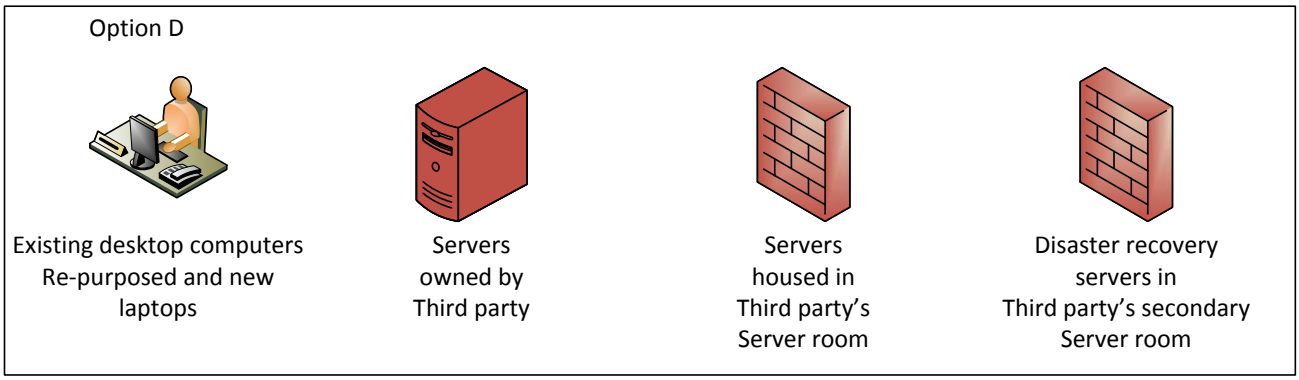
Type of Expenditure	Year 1		Year 2		Year 3		Year 4		Year 5		Total	
	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue
	£	£	£	£	£	£	£	£	£	£	£	£
Investments												
Broadband	5,000	5,430	0	5,540	0	5,650	0	5,770	0	5,880	5,000	28,270
IT Licenses / Agreements	0	105,430	0	105,590	0	105,750	0	105,910	0	106,080	0	528,760
ICT Contract	0	31,780	0	32,310	0	32,960	0	33,620	0	34,290	0	164,960
Hardware	389,720	0	4,500	0	3,500	0	24,100	0	12,500	0	434,320	0
Software	84,910	0	0	0	0	0	0	0	0	0	84,910	0
Professional Fees	568,200	0	0	0	0	0	0	0	0	0	568,200	0
Total	**£1,047,830**	**£142,640**	**£4,500**	**£143,440**	**£3,500**	**£144,360**	**£24,100**	**£145,300**	**£12,500**	**£146,250**	**£1,092,430**	**£721,990**
Total plus 2% contingency	**£1,073,080**	**£146,080**	**£4,610**	**£146,900**	**£3,580**	**£147,840**	**£24,680**	**£148,800**	**£12,800**	**£149,770**	**£1,118,750**	**£739,390**
Savings												
Security	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(13,000)
IT Licenses / Agreements	0	(5,980)	0	(5,980)	0	(5,980)	0	(5,980)	0	(5,980)	0	(29,900)
ICT Contract	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(180,000)
Total	**£0**	**(£44,580)**	**£0**	**(£44,580)**	**£0**	**(£44,580)**	**£0**	**(£44,580)**	**£0**	**(£44,580)**	**£0**	**(£222,900)**
Grand Total	**£1,073,080**	**£101,500**	**£4,610**	**£102,320**	**£3,580**	**£103,260**	**£24,680**	**£104,220**	**£12,800**	**£105,190**	**£1,118,750**	**£516,490**

H.1.11 The costs of Option C1 are:

Type of Expenditure	Year 1		Year 2		Year 3		Year 4		Year 5		Total	
	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue
	£	£	£	£	£	£	£	£	£	£	£	£
Investments												
IT Licenses / Agreements	0	7,000	0	7,140	0	7,280	0	7,430	0	7,580	0	36,430
Hardware	32,100	0	14,500	0	3,500	0	24,100	0	12,500	0	86,700	0
Software	73,580	0	0	0	0	0	0	0	0	0	73,580	0
Professional Fees	695,300	171,600	0	174,480	0	177,970	0	181,530	0	185,160	695,300	890,740
Total	**£800,980**	**£178,600**	**£14,500**	**£181,620**	**£3,500**	**£185,250**	**£24,100**	**£188,960**	**£12,500**	**£192,740**	**£855,580**	**£927,170**
Total plus 2% contingency	**£820,280**	**£182,900**	**£14,850**	**£186,000**	**£3,580**	**£189,710**	**£24,680**	**£193,510**	**£12,800**	**£197,390**	**£876,190**	**£949,510**
Savings												
Electricity	0	(10,000)	0	(10,000)	0	(10,000)	0	(10,000)	0	(10,000)	0	(50,000)
Security	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(13,000)
IT Licenses / Agreements	0	(6,930)	0	(6,930)	0	(6,930)	0	(6,930)	0	(6,930)	0	(34,650)
ICT Contract	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(180,000)
Total	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£277,650)**
Grand Total	**£820,280**	**£127,370**	**£14,850**	**£130,470**	**£3,580**	**£134,180**	**£24,680**	**£137,980**	**£12,800**	**£141,860**	**£876,190**	**£671,860**

H.1.12 The costs of Option C2 are:

Type of Expenditure	Year 1		Year 2		Year 3		Year 4		Year 5		Total	
	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue
	£	£	£	£	£	£	£	£	£	£	£	£
Investments												
IT Licenses / Agreements	0	116,080	0	116,450	0	116,830	0	117,220	0	117,610	0	584,190
ICT Contract	0	31,780	0	32,310	0	32,960	0	33,620	0	34,290	0	164,960
Hardware	288,890	0	14,500	0	3,500	0	24,100	0	12,500	0	343,490	0
Software	84,910	0	0	0	0	0	0	0	0	0	84,910	0
Professional Fees	578,200	0	0	0	0	0	0	0	0	0	578,200	0
Total	**£952,000**	**£147,860**	**£14,500**	**£148,760**	**£3,500**	**£149,790**	**£24,100**	**£150,840**	**£12,500**	**£151,900**	**£1,006,600**	**£749,150**
Total plus 2% contingency	**£974,940**	**£151,420**	**£14,850**	**£152,350**	**£3,580**	**£153,400**	**£24,680**	**£154,480**	**£12,800**	**£155,560**	**£1,030,850**	**£767,210**
Savings												
Electricity	0	(10,000)	0	(10,000)	0	(10,000)	0	(10,000)	0	(10,000)	0	(50,000)
Security	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(13,000)
IT Licenses / Agreements	0	(6,930)	0	(6,930)	0	(6,930)	0	(6,930)	0	(6,930)	0	(34,650)
ICT Contract	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(180,000)
Total	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£277,650)**
Grand Total	**£974,940**	**£95,890**	**£14,850**	**£96,820**	**£3,580**	**£97,870**	**£24,680**	**£98,950**	**£12,800**	**£100,030**	**£1,030,850**	**£489,560**



H.1.8 Option D rents space from another company and uses space in their server room. This means that the cost of owning, running and replacing the equipment is with another organisation. The implication is that there is a lower up-front cost; however the ongoing cost is increased to provide a monthly billing structure.

H.1.9 The Council has utilised this technology for many years with specific products such as those listed below:

- Finance and procurement system looked after by Solihull MBC,
- HR and payroll system hosted by Stafford Borough Council,
- Both the new CRM and the old LG-45 CRM,
- The Garrick Theatre's ticket booking system,
- The Contact Centre used by Lichfield Connects and the corporate telephone system,
- Income management and electronic payments tools,
- Covalent Performance Management,
- Objective, formerly Limehouse, Local Plan development tool,
- Bartec, the in-cab waste management service.

H.1.10 The advantages and disadvantages of this option are:

- Advantages:
  - Less up-front investment required
  - Uses robust server rooms designed for purpose
  - Business continuity designed from the start
  - Gives ability to support future strategy
  - Only option that gives cost saving from reduced insurance
- Disadvantages:
  - Infrastructure more complicated as more companies are involved
  - Risk of losing control and reliance on strong contract management
  - More on going revenue money required

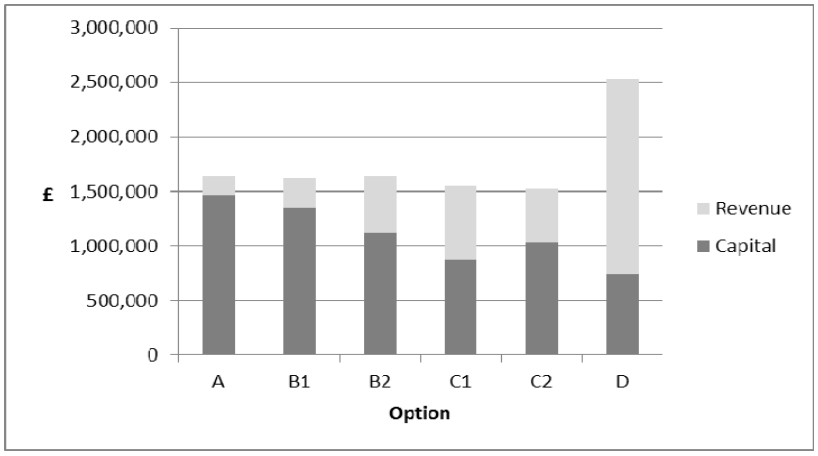
H.1.11 The costs of Option D are:

Type of Expenditure	Year 1		Year 2		Year 3		Year 4		Year 5		Total	
	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue	Capital	Revenue
	£	£	£	£	£	£	£	£	£	£	£	£
Investments												
IT Licenses / Agreements	0	7,000	0	7,140	0	7,280	0	7,430	0	7,580	0	36,430
Hardware	32,100	0	14,500	0	3,500	0	24,100	0	12,500	0	86,700	0
Software	57,720	0	0	0	0	0	0	0	0	0	57,720	0
Professional Fees	577,300	380,520	0	388,130	0	395,890	0	403,810	0	411,890	577,300	1,980,240
Total	**£667,120**	**£387,520**	**£14,500**	**£395,270**	**£3,500**	**£403,170**	**£24,100**	**£411,240**	**£12,500**	**£419,470**	**£721,720**	**£2,016,670**
Total plus 2% contingency	**£683,200**	**£396,860**	**£14,850**	**£404,800**	**£3,580**	**£412,890**	**£24,680**	**£421,150**	**£12,800**	**£429,580**	**£739,110**	**£2,065,280**
Savings												
Electricity	0	(10,000)	0	(10,000)	0	(10,000)	0	(10,000)	0	(10,000)	0	(50,000)
Security	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(2,600)	0	(13,000)
IT Licenses / Agreements	0	(6,930)	0	(6,930)	0	(6,930)	0	(6,930)	0	(6,930)	0	(34,650)
ICT Contract	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(36,000)	0	(180,000)
Total	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£55,530)**	**£0**	**(£277,650)**
Grand Total	**£683,200**	**£341,330**	**£14,850**	**£349,270**	**£3,580**	**£357,360**	**£24,680**	**£365,620**	**£12,800**	**£374,050**	**£739,110**	**£1,787,630**

H.2 Costs of the recommendations

H.2.1 A comprehensive cost model has been developed for each of the options. The summary costs for each of the options are shown in the table and graph below:

Option	Year 1		Year 2		Year 3		Year 4		Year 5		Total		Total
	Capital £	Revenue £	Capital £	Revenue £	Capital £	Revenue £	Capital £	Revenue £	Capital £	Revenue £	Capital £	Revenue £	£
LDC's equipment in LDC's server room													
A	£1,192,690	£30,240	£46,310	£35,100	£33,690	£36,090	£66,160	£37,110	£127,090	£38,140	**£1,465,940**	**£176,680**	**£1,642,620**
B1	£1,299,190	£51,360	£4,610	£53,020	£3,580	£54,960	£24,680	£56,970	£12,800	£58,990	**£1,344,860**	**£275,300**	**£1,620,160**
B2	£1,073,080	£101,500	£4,610	£102,320	£3,580	£103,260	£24,680	£104,220	£12,800	£105,190	**£1,118,750**	**£516,490**	**£1,635,240**
LDC's equipment in third party server room													
C1	£820,280	£127,370	£14,850	£130,470	£3,580	£134,180	£24,680	£137,980	£12,800	£141,860	**£876,190**	**£671,860**	**£1,548,050**
C2	£974,940	£95,890	£14,850	£96,820	£3,580	£97,870	£24,680	£98,950	£12,800	£100,030	**£1,030,850**	**£489,560**	**£1,520,410**
Third party equipment in third party server room													
D	£683,200	£341,330	£14,850	£349,270	£3,580	£357,360	£24,680	£365,620	£12,800	£374,050	**£739,110**	**£1,787,630**	**£2,526,740**



H.2.2 The cost model shows that option C2 has the lowest overall cost over a five year period. This option is to put equipment purchased by the Council through a Staffordshire County Council framework into the Staffordshire County Council server rooms.

H.2.3 This option is more cost effective than keeping equipment in the Council's server room as the cost Staffordshire County Council have quoted is comparable to the current running cost of the Council's server room. This means the Council will not need to make significant investment in bringing the existing Council server room to the required specification and building a second server room at an alternative Council premise.

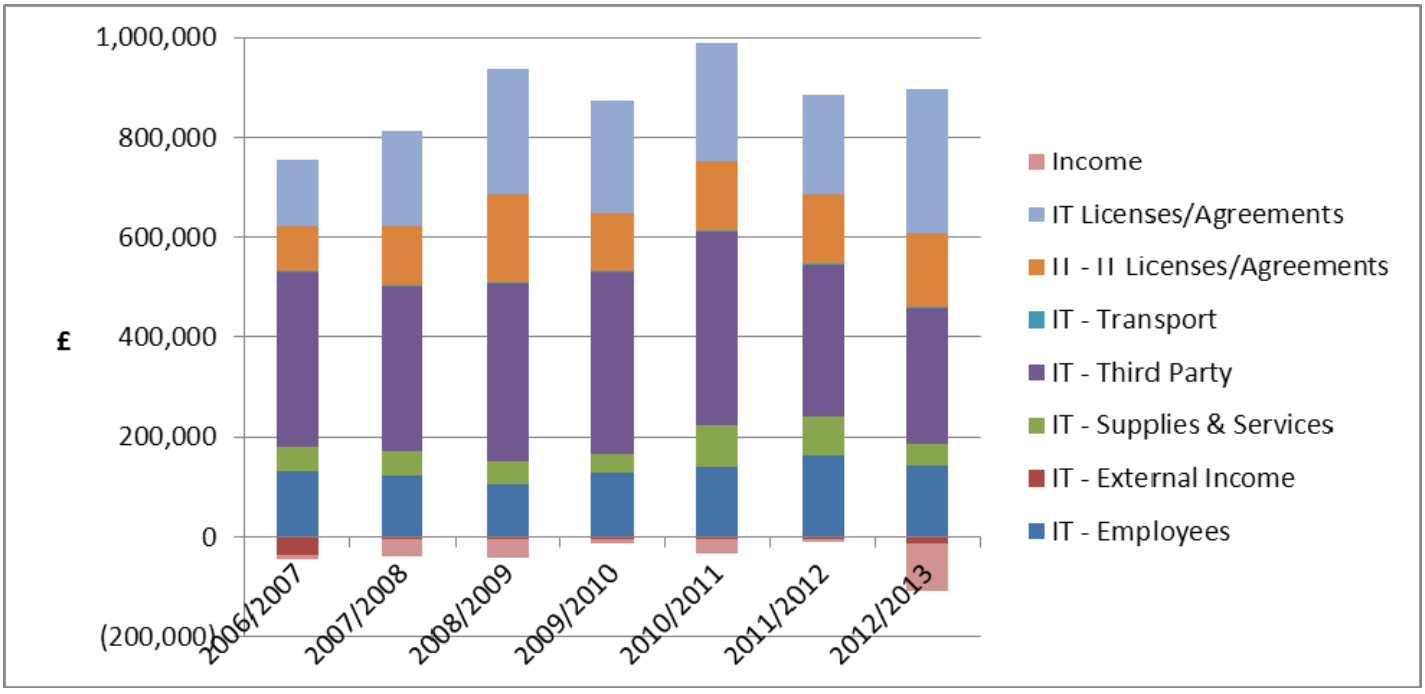
H.2.4 Also this option is more cost effective than using the ICT support provider's server room as it reuses the existing investment with Staffordshire County Council and their communications links that connect each Council premise together and the to the Internet. This means that this option achieves one of the key outcomes of the project by having disaster recovery built in at the beginning. Currently if the network connection to the Council's server room gets broken only the Frog Lane offices will continue to work. If this were to occur with option C2 in the future then only the Frog Lane offices would be disconnected.

H.2.5 This option also allows the Council to review its ICT support in 2017 when the first term of the current contract ends. The risk of expensive exit plans is largely avoided as the cost of the ANS Group supporting the solution has been factored into the model.

I.1 The cost of ICT to the Council

I.1.1 As part of the review the cost of ICT to the Council has been review and the table below shows

ICT	2006/2007 £	2007/2008 £	2008/2009 £	2009/2010 £	2010/2011 £	2011/2012 £	2012/2013 £	Total £
Costs attributed to ICT team								
IT - Employees	129,610	122,680	105,520	126,910	138,110	160,000	142,570	**925,390**
IT - External Income	(38,670)	(4,130)	(4,490)	(4,510)	(5,320)	(4,520)	(13,060)	**(74,700)**
IT - Supplies & Services	50,830	50,780	43,750	40,770	83,650	79,130	42,930	**391,840**
IT - Third Party	349,680	326,890	357,530	360,780	388,740	302,840	273,040	**2,359,490**
IT - Transport	2,500	1,920	2,670	4,560	3,060	3,030	2,060	**19,810**
IT - IT Licenses/ Agreements	87,940	118,920	175,540	113,610	136,300	139,850	145,750	**917,900**
Total	**581,890**	**617,060**	**680,520**	**642,130**	**744,540**	**680,320**	**593,290**	**4,539,740**
Other ICT costs								
IT Licenses/ Agreements	135,990	191,280	250,750	226,600	239,700	199,060	289,500	**1,532,870**
Income	(9,160)	(35,470)	(40,080)	(8,260)	(26,740)	(5,000)	(96,220)	**(220,910)**
Total	**£708,720**	**£772,870**	**£891,190**	**£860,470**	**£957,490**	**£874,390**	**£786,570**	**£5,851,690**



I.1.2 This analysis shows the cost of the ICT team rose between 2006/2007 and 2010/2011 however, since then has reduced by around £152,000 per year. The cost last year was around 1.8% higher than 2006/2007 in spite of the increasing demands from the Public Sector Network and compliance checks from companies such as Microsoft, Adobe and Oracle.

J.1 The outcome from implementing these recommendations

J.1.1 Implementing the recommendations made in this report will fix many of the problems the Council is experiencing with its ICT. It will undoubtedly generate new challenges and these will need to be addressed through the project governance structure.

J.1.2 It is important to understand how this will change the opportunities for the Council. Ultimately the Council needs to focus on the data it holds and getting the maximum value from it rather than managing servers and desktops. There are companies such as the ANS Group who specialise in looking after the equipment and taking away the management overhead from their customers.

J.1.3 The outcome from the project is a modern environment capable of supporting the demands of its many users. But, it is more than just that, the environment proposed will assist in preventing this scenario happening in the future. This section describes how this will be avoided for the IT challenges the Council is currently facing

J.2 Avoiding these challenges in the future

J.2.1 Microsoft will end support for Windows 7 and Office 2013 at some point in the future and in order to avoid this becoming an issue in the future the new environment enables new software applications to be rolled out in a controlled and centralised manner. This means that it will be possible for new versions of Windows or Microsoft Office to be tested alongside the existing versions. By making it easier to roll out and withdraw new versions of software applications it will make it easier to move to them and not have to be such large scale projects. The Council will simply be able to reap the reward of the investment by being ready to make changes.

J.2.2 In most cases it is anticipated that the new environment will separate the operating system from the desktop computers. The role of the desktop computer will be to display the pictures on the screen and to interpret key presses and mouse moves as all of the processing is undertaken by the central servers. By splitting the hardware from the operating system it means that the hardware becomes less relevant and no longer needs to be a desktop computer. With the current investment in Citrix the Council's applications have been accessed on smartphones, tablets and Apple Macintosh computers without having to be concerned about the actual physical device. As tablets mature then this investment will help the Council to prepare for the opportunities for mobile and remote working.

J.2.3 The proposed environment uses established IT techniques so it means that new servers can be brought into service very quickly without the need to necessarily buy new hardware for it to sit on. The vision is that creating a new server should be almost as easy as choosing the features the server needs from a menu and it appearing. This means that the issues with the age of the hardware becoming irrelevant.

J.2.4 The environment itself will need to be upgraded or replaced as time progresses, this iteration of it is based on a five year model. At the end of the five years there will be investment required, but it will give an opportunity to review how this has worked and how the IT market has changed over those give years.

J.2.5 By placing the environment in the County Council server rooms as with the environment itself, it places the management in the hands of specialists who will ensure that the room is fit for purpose and meets the needs of the equipment housed within it.

J.2.6 The investment the County Council has made in server rooms is far greater than the District Council would be able to and this will assist with the Business Continuity Solution. The environment has Business Continuity built in from the beginning as opposed to being added on and this will enable regular testing and ensuring that data can be recovered should the worst happen. This is further enhanced supported by the investment the Council has made with the County Council in data links as each of the Council's premises are individually connected to the County Council, meaning there is less reliance on one single site as there is.

J.2.7 The Cabinet Office has taken local authorities on a journey to improve their security and while they may seem overly bureaucratic ultimately they serve to protect the information the Council holds about citizens and businesses. It is not possible to fully appreciate where the journey will take the Council but it is anticipated that in implementing the additional security equipment it will go a long way to creating the safe environment that is needed.

Information, Communications and Technology Access, Use and Security Policy

K.1.1 Introduction

K.1.1.1 We need to keep our Information, Communications and Technology (ICT), the customer information and how we exchange information with other organisations safe and secure.

K.1.1.2 The information that we hold, process, maintain and share with others is an important asset and like other important business assets needs to be suitably protected. All information has a value, however, not all of this information has an equal value or requires the same level of protection.

K.1.1.3 So we can build public confidence and make sure we comply with the relevant statutory legislation, it is vital that we maintain the highest standards of information security. To help in doing this a policy has been put in place.

K.1.1.4 This policy applies to anyone who has access to our information systems or our information of any type or format (paper or electronic).

K.1.1.5 Everyone has a role to play and a contribution to ensure the safe and secure use of technology and the information that as information security cannot be achieved by technical means alone. Non-compliance with this policy could have a significant effect on our operations and may result in financial loss and an inability to provide necessary services to our customers.

K.1.1.6 The misuse of our computer and telephony resources is considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action including dismissal.

K.1.2 Purpose

K.1.2.1 This document provides a summary of the policy that has been developed. The objective of the policy is to ensure that we keep our computers and information safe and secure at all times so that:

- The public and anyone who uses our information systems are confident of the confidentiality, integrity and availability of the information used and produced.
- Business damage and interruption caused by security incidents are minimised.
- All legislative and regulatory requirements are met.
- The ICT equipment and facilities are used responsibly, securely and with integrity at all times.

K.1.2.2 The policy we have developed are based on industry good practice and intend to satisfy the requirements set out by the Public Sector Network Code of Connection (CoCo). The policy includes:

- Information Protection,
- Accessing systems,
- Routine Operations,
- Computer, telephone and desk use,
- Email usage,
- Information Security Incident Management,
- Internet usage,
- ICT infrastructure,
- Remote working,
- Removable media,
- Social media usage,
- Software.

K.1.2.3 The purpose of each section of the policy along with key messages are summarised as:

K.1.3 Information Protection

K.1.3.1 We will ensure the protection of all information assets within our custody. High standards of confidentiality, integrity and availability of information will be maintained at all times.

K.1.3.2 Key Messages

- We must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the Government Security Classifications Policy (GSCP).
- OFFICIAL information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Where secure email is available to connect the sender and receiver of the email message, this must be used for all external email use and must be used for communicating OFFICIAL material.
- The disclosure of OFFICIAL classified information in any way other than via secure email is a disciplinary offence.

K.1.4 Accessing systems

K.1.4.1 We have established specific requirements for protecting information and information systems against unauthorised access. We will effectively communicate the need for information and information system access control.

K.1.4.2 Key Messages

- Everyone must use strong passwords.
- Passwords must be protected at all times and must be changed at least every 90 days.
- Your access rights must be reviewed at regular intervals.
- It is your responsibility to prevent your username and password being used to gain unauthorised access to our systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the network without permission from the ICT team.
- Partners or 3rd party suppliers must contact the IT helpdesk before connecting to the network.

K.1.5 Routine Operations

K.1.5.1 We will ensure the protection of our IT service (including any information systems and information processing equipment used by the organisation) against malware and malicious and mobile code. Only authorised changes will be made to the IT service (including any information systems and information processing equipment). Information leakage will be prevented by secure controls.

K.1.5.2 Key Messages

- Changes to the operating systems must follow the formal change control procedure.
- Appropriate access controls shall be put in place to prevent the installation of software and to protect against malicious and mobile code.
- Regular backups of essential business information will be taken to ensure that we can recover from a disaster, media failure or error.
- Storage media must be handled, protected and disposed of with care.
- Connections to the network are made in a controlled manner.
- An annual health check must be made of all IT infrastructure systems.

K.1.6 Computer, Telephone and Desk Use

K.1.6.1 We will ensure that everyone is aware of, and understands, the acceptable use of our computer and telephony resources and the need to ideally operate within a “clear desk” environment.

K.1.6.2 Key Messages

- You must adhere to the Telephone Acceptable Use Procedure / Code of Practice at all times.
- You must ideally maintain a clear desk at all times.
- OFFICIAL information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

K.1.7 Email

K.1.7.1 We will ensure everyone is aware of the acceptable use of our email facilities.

K.1.7.2 Key Messages

- All emails that are used to conduct or support official business must be sent using a corporate email address.
- All emails sent via the Public Sector Network must have a secure email address.
- Non-work email accounts must not be used to conduct or support official business or transmit the organisations owned documents.
- Everyone must ensure that any emails containing sensitive information must be sent from an official business email.
- All official external e-mail must carry the official disclaimer.
- Under no circumstances must you communicate material (either internally or externally), that is defamatory, obscene, or does not comply with the Equal Opportunities procedure.
- Where secure email is available to connect the sender and receiver of the email message, this must be used for all external email use and must be used for communicating OFFICIAL material.
- Automatic forwarding of email must be considered carefully to prevent OFFICIAL material being forwarded inappropriately.
- Where possible do not use a business email address for personal use.

K.1.8 Information Security Incident Management

K.1.8.1 We will ensure that we react appropriately to any actual or suspected incidents relating to information systems and information within the custody of the organisation.

K.1.8.2 Key Messages

- All staff must report any incidents or suspected incidents immediately by contacting the IT helpdesk.
- We can maintain your anonymity when reporting an incident if you wish.

K.1.9 Internet Acceptable Usage

K.1.9.1 We will ensure everyone is aware of the acceptable use of our internet facilities.

K.1.9.2 Key Messages

- You must familiarise themselves with the detail, essence and spirit of this section before using the Internet facility provided.
- At the discretion of line manager, and provided it does not interfere with work, you can access the internet for personal use outside of working hours (for example during your lunch-break).
- You must not create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.
- You must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

K.1.10 ICT Infrastructure

K.1.10.1 There shall be no unauthorised access to either physical or electronic information within the custody of the organisation. This includes sensitive paper records, IT equipment used to access electronic data and IT equipment used to access the network.

K.1.10.2 Key Messages

- OFFICIAL information, and equipment used to store and process this information, must be stored securely.
- Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by the ICT team, as appropriate. Keys are not stored near these secure areas or lockable cabinets.

- All general computer equipment must be located in suitable physical locations.
- Desktop PCs must not have data stored on the local hard drive.
- Non-electronic information must be assigned an owner and a classification. OFFICIAL information must have appropriate information security controls in place to protect it.
- Staff must be aware of their responsibilities in regard to the Data Protection Act.
- Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed.

K.1.11 Remote Working

K.1.11.1 We provide you with the facilities and opportunities to work remotely as appropriate. We will ensure that all employees who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.

K.1.11.2 Key Messages

- It is your responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention when moving portable computer devices and not emailing OFFICIAL information to a non-business email address.
- You need to be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- It is your responsibility to ensure that access to all OFFICIAL information is controlled – e.g. through password controls.
- All OFFICIAL data held on portable computer devices must be encrypted.

K.1.12 Removable Media

K.1.12.1 We will ensure the controlled use of removable media devices to store and transfer information by anyone who has access to information, information systems and IT equipment for the purposes of conducting official business.

K.1.12.2 Key Messages

- We control the use of removable media devices. The use of removable media devices will only be approved if there is a valid business case for its use.
- Any removable media device that has not been supplied by ICT must not be used.
- All data stored on removable media devices must be encrypted where possible.
- Damaged or faulty removable media devices must not be used and returned to ICT for secure disposal.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices are not for personal use.

K.1.13 Social Media Usage

K.1.13.1 We will ensure everyone is aware of the acceptable use of both business and personal social media facilities.

K.1.13.2 Key Messages

- Be:
  - Credible, accurate, fair, thorough and transparent.
  - Consistent, cordial, honest and professional at all times.
  - Responsive, social media is like a public discussion forum. Respond as soon as you can, otherwise it will reflect badly on the service/organisation if you leave a question unanswered for a long period of time.
  - Integrated - Wherever possible align online participation with other offline communications (press releases, leaflets etc.)
  - A responsible officer Remember that you are an ambassador for the organisation and the code of conduct still applies in your leisure time.

K.1.14 Software

K.1.14.1 We will ensure the acceptable use of software by everyone using the organisation's computer equipment or Information Systems.

K.1.14.2 Key Messages

- All software acquired must be purchased through the ICT team.
- Under no circumstances is any personal or unsolicited software be loaded onto a business machine.
- Every piece of software is required to have a licence and we will not condone the use of any software that does not have a licence.
- Unauthorised changes to software must not be made.
- You are not permitted to bring software from home (or any other external source) and load it onto our computers.
- You must not attempt to disable or reconfigure the Personal Firewall software.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

K.1.15 Compliance

K.1.15.1 If anyone is found to have breached this policy, they may be subject to the disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

K.1.15.2 If you do not understand the implications of this policy or how it may apply to you, please seek advice from ICT.

K.1.16 Risks

K.1.16.1 This policy aims to address the risks associated with accessing and handling information in order to conduct our official business. Examples of the risks we are trying to mitigate include:

- Contamination of ICT networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Data leakage.
- Disclosure of OFFICIAL information as a consequence of loss, theft or careless use of removable media devices.
- Incorrect transmission method i.e. not using secure email.
- Inadequate destruction of data.
- Increased risk of equipment damage, loss or theft.
- Potential sanctions against the organisation or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the organisation or individuals as a result of information loss or misuse.
- Reputational damage as a result of information loss or misuse.
- The loss of direct control of peoples' access to information systems and facilities.
- The non-reporting of information security incidents.
- To reduce the impact of information security breaches by ensuring incidents are followed up correctly.
- To help identify areas for improvement to decrease the risk and impact of future incidents.
- Unauthorised access to OFFICIAL information.
- Unauthorised introduction of malicious software and viruses.
- Virus transmission.

K.1.16.2 Non-compliance with this policy could have a significant effect on the efficient operation of the business and may result in financial loss and an inability to provide necessary services to our customers.

K.1.17 Legislation

K.1.17.1 You must understand the relevant legislation relating to Information Security and Data Protection, and must be aware of your responsibilities under this legislation. The following statutory legislation governs aspects of the organisation's information security arrangements. This list is not exhaustive:

- Freedom of Information Act 2000.
- Human Rights Act 1998.
- Electronic Communications Act 2000.
- Regulation of Investigatory Powers Act 2000.
- Data Protection Act 1998.
- Copyright Designs and Patents Act 1988.
- Computer Misuse Act 1990.
- Environmental Information Regulations 2004.
- Re-use of Public Sector Information Regulations 2005.

K.1.17.2 Individuals can be held personally and legally responsible for breaching the provisions of the above Acts.

K.1.18 Personal Security Declaration

K.1.18.1 The first stage of gaining access to our IT systems is to sign a personal security declaration. This section covers the personal commitments you are making by signing the security declaration.

- ✓ I acknowledge that my use of any IT system and network may be monitored and/or recorded for lawful purposes.
- ✓ I agree to be responsible for any use by me of any usernames, passwords, access tokens or other mechanism as provided that I am given.
- ✓ I will:
  - ✓ Comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant.
  - ✓ Inform my manager and the ICT helpdesk immediately if I detect, suspect or witness an incident that may be a breach or potential breach of data security.
  - ✓ Make myself familiar with the security policies, procedures and any special instructions that relate to individual IT systems or networks.
  - ✓ Protect such credentials at least to the same level of Protective Marking as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure approved location at my employer's premises).
  - ✓ Protect any material, whatever the sensitivity or protective marking, sent, received, stored or processed by me to the same level as I would paper copies of similar material.
  - ✓ Securely store or destroy any printed material or other hard copies.
  - ✓ Seek to prevent inadvertent disclosure of information by avoiding being overlooked when working, by taking care when printing information (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted.
  - ✓ Take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief).
- ✓ I will not:
  - ✓ Attempt to access any data that I have not been given explicit permission to access.
  - ✓ Attempt to access the IT systems or networks other than from IT systems and locations that I have been explicitly authorised to use for this purpose.

- ✓ Attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.
- ✓ Disable anti-virus protection provided at my computer.
- ✓ Disclose information other than on a 'need to know' basis.
- ✓ Introduce viruses, Trojan horses or other malware into the IT systems or networks.
- ✓ Leave my computer unattended in such a state as to risk unauthorised disclosure of information stored in, processed by, or transmitted by any IT systems or networks.
- ✓ Make false claims or denials relating to my use of any IT systems or networks (e.g. falsely denying that an entry had been made or altered, also any content uploaded / downloaded).
- ✓ Remove equipment or information from my employer's premises without appropriate approval.
- ✓ Send information marked OFFICIAL using any method unless I have been expressly authorised by my line manager to do so.
- ✓ Use a colleague's credentials to access any IT systems or networks and will equally ensure that my credentials are not shared and are protected against misuse.

- ✓ Where my organisation has implemented other measures to prevent unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection;
- ✓ If I am about to leave or change role, I will inform my Line Manager prior to departure of any information held in my account.

K.2 Information Protection

K.2.1 Definition

K.2.1.1 Information classification puts information into categories depending on the harm that could result from the loss or unauthorised disclosure. On creation, all information assets much be assessed to determine the appropriate classification category.

K.2.1.2 Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that we maintain. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper,
- Data stored electronically,
- Communications sent by post / courier or using electronic means,
- Stored tape or video,
- Speech.

K.2.1.3 This section details the basic requirements and responsibilities for the proper management of our information assets and the means of information handling and transfer.

K.2.2 Identifying Information Assets

K.2.2.1 The first step in managing information is to identify the important information assets and this must be sensible and pragmatic. Information assets are not only ICT systems and can be any in format e.g. paper, electronic, or microfilm. To assess whether something is an information asset consider whether:

- It has value to the organisation
- It would cost money to re-acquire
- There would be legal, reputational or financial repercussions if it could not be produced on request
- It would affect operational efficiency if it can be accessed easily

- There are risks associated with its loss, inaccuracy or inappropriate disclosure.

K.2.2.2 There must be an inventory of all important information assets that we rely upon. It will identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. At minimum it must include the following:

- Type,
- Location,
- Designated owner,
- Security classification,
- Format,
- Backup,
- Licensing information.

K.2.3 Classifying Information

K.2.3.1 On creation and where software to hold the classification exists, all information assets must be assessed and classified by the owner according to their content. At minimum all information assets must be classified and labelled in accordance with the Government Security Classifications Policy (GSCP). The classification will determine how the document must be protected and who is allowed access to it. Any system subsequently allowing access to this information must clearly indicate the classification. Information up to OFFICIAL sent via the Public Sector Network must be labelled appropriately using the GSCP guidance.

K.2.3.2 The GSCP requires information assets to be protectively marked into one of three classifications. The way the document is handled, published, moved and stored will be dependent on this scheme.

K.2.3.3 The classes are:

- OFFICIAL,
- SECRET,
- TOP SECRET.

K.2.3.4 In addition there are descriptors to help identify the type of information and these are listed later in this section.

K.2.3.5 The method of classifying information risks using a risk based approach to determine the classification level is later in this section, but it has been deemed by Government that the only data held is rated at OFFICIAL.

K.2.4 Assigning Asset Owners

K.2.4.1 All important information assets must have a nominated owner and need to be accounted for. An owner must be an employee whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it must be formalised and agreed. For information assets whose use throughout the business is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This must be the person who has the most control over the information. In the case of ICT systems where the administration has been devolved from ICT the asset owner will also be the system owner and responsible for signing the system owner agreement.

K.2.5 Unclassified Information Assets

K.2.5.1 Items of information that have no security classification and are of limited or no practical value must not be assigned a formal owner or inventoried. Information needs to be destroyed if there is no legal or operational need to keep it and temporary owners need to be assigned within each department to ensure that this is done.

K.2.6 Information Assets with Short Term or Localised Use

K.2.6.1 For new documents that have a specific, short term localised use, the creator of the document will be the originator. This includes letters, spreadsheets and reports created by staff. All staff must be informed of their responsibility for the documents they create.

K.2.7 Information Storage and access

K.2.7.1 All electronic information will be stored on centralised facilities to allow regular backups to take place. Where it has been defined records management and retention guidance must be followed.

K.2.7.2 Staff must not be allowed to access information until their line manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

K.2.7.3 It is the responsibility of information owners who have databases holding personal information to create a defined security and system management procedure for the records and documentation. This documentation will include a clear statement as to the use, or planned use of the personal information.

K.2.8 Sharing Information

K.2.8.1 OFFICIAL information must not be disclosed to any other person or organisation via any insecure method including, but not limited, to paper based methods, fax and telephone.

K.2.8.2 Where information is disclosed/shared it must only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.

K.2.8.3 Disclosing OFFICIAL information to any external organisation is also prohibited, unless via the Public Sector Network email. For further information see the section on Email usage.

K.2.8.4 The disclosure of OFFICIAL information in any way other than via secure email is a disciplinary offence. If there is suspicion of anyone treating OFFICIAL information in a way that could be harmful to the organisation or to the data subject, then it is to be reported to the ICT team, and the person may be subject to disciplinary procedure.

K.2.8.5 Any sharing or transfer of information with other organisations must comply with all Legal, Regulatory and organisational requirements. In particular this must be compliant with the Data Protection Act 2000, The Human Rights Act 2000 and the Common Law of Confidentiality.

K.2.8.6 Even if you come across information that is assessed as unclassified, such as historical documents, you must not disclose these by any means such as emailing them or posting them to websites without first seeking the approval of the asset owner and/or the Legal section.

K.2.9 Information Classification Approach

K.2.9.1 Classifying information assets has to be a combination of both training and technology. An email containing a list of credit card numbers with just the 16 digits may be given a low classification, however if that list also contained expiry dates or some other information about the credit card holder the security classification would increase as there is a greater impact to the business if the data is lost.

K.2.9.2 The table below gives guidance on the how to treat the classification that must be applied to an asset.

	OFFICIAL		
	OFFICIAL with no sensitive information	**OFFICIAL with minor sensitive information about one individual**	**OFFICIAL with sensitive information about multiple individuals**
Protective marking	Not sensitive,	Information that	Information that

	including items that may not be for external circulation; internal memos, minutes, project reports etc.	could cause significant harm to an individual, the organisation, apprehension of an offender or public affairs	would damage or prejudice an individual, the organisation, apprehension of an offender or public affairs
Internal dispatch	Sealed envelope / packaging showing protective mark		
Post or Courier	Sealed envelope / packaging - no protective mark or identifiable descriptor		
Telephone	Care must be taken to establish the identity of the caller	Use of telephone must be avoided where possible, but if absolutely necessary the identity of the other party must be established before disclosure	
Fax	Care must be taken to ensure the correct number is dialled	Use of fax must be avoided, but if absolutely necessary then steps must be taken to ensure the recipient is at the fax machine and confirms receipt	
Email – Internal or secure email	Can be sent in accordance with the Email usage section of this document		
Email - External	No encryption required	Use a secure email account where possible. Where recipient does not have access to secure email use External Encryption descriptor. For more details contact ICT.	
Clear Desk	Left tidily as per policy	All documents must be locked away when not at desk	
Disposal	Normal recycling facilities to be used for general paper waste	Dispose of documents using secure shredding facilities	

K.2.9.3 In addition to choosing the top level heading a descriptor will need to be chosen to help classify the subject of the data. The table below shows the descriptors we use and also a selection of documents that would apply to each descriptor.

Descriptor	**Document Type**	**Additional Details**
Organisational	Reports	
	Minutes	
	Agendas	
	Policies	
	Procedures	
	Strategies	
	Business Plans	
	Performance Plans	
	Action Plans	
	Performance Indicators	
	FOI Requests	
	Invoices	
	Statutory returns	

Descriptor	Document Type	Additional Details
	Budget Monitoring	
	Payment Details	
	Income / Expenditure	
	Contract payments	
	Contracts	
	SLAs	
	Legal advice	
	Agreements	
Personal	Employee employment details	Includes combinations of name, address, telephone number, job and bank account details
	Employee personal details	
	Customer personal details	
	Disciplinary / Investigation	
	Health and Safety Accident Forms	
	Sickness absence	Employee and Client
	Appointments	
	Individual Sickness Records	
	Medical History	
External Encryption	Information that is classed as OFFICIAL or above that needs to be sent to a non-secure email account as a one off instance	Sender will be required to make contact, separate to that made by email, in order to provide the recipient with the relevant access
External Encryption – Regular Recipient	Information that is classed as OFFICIAL or above that needs to be sent to a non-secure email account on a regular occurrence i.e. Bromford Housing	Receiver will be required to create their own 'account' in order to receive the encrypted email

K.3 Accessing systems

K.3.1 Purpose

K.3.1.1 We need to protect our information against accidental or malicious disclosure, modification or destruction. We use access controls to protect information by controlling who has access to use different information resources and by guarding against unauthorised use.

K.3.1.2 This section explains how we will check that individuals are authorised to access to information is granted, how access is regularly reviewed and how such access is removed promptly when the need to have access ends. This section also addresses third party access to corporate information systems (e.g. contractors, service providers, voluntary agencies and partners).

K.3.2 Employee Access to the network – Prior to employment

K.3.2.1 We must ensure that potential people accessing the network are recruited in line with the organisation's recruitment procedure for the roles they are considered for and to reduce the risk of theft, fraud or misuse of information or information systems by those people. These requirements are corporate in nature.

K.3.2.2 Background verification checks must be carried out on all potential employees, in accordance with all relevant laws, regulations and ethics. The level of such checks must be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved. For further information on the basic requirements for employment contact the Personnel team.

K.3.2.3 If an employee requires access to OFFICIAL information or the Public Sector Network they must be cleared to "Baseline Personnel Security Standard". The following requirements must be met:

- ✓ Minimum of two satisfactory references,
- ✓ Completeness and accuracy check of employee's application form,
- ✓ Confirmation of claimed academic and professional qualifications,
- ✓ Identity check against a passport or equivalent document that contains a photograph. Identity must be proven through visibility of:
  - ✓ A full ten year passport,
  - ✓ Or two from the following list:
    - ✓ British driving licence.
    - ✓ P45 form.
    - ✓ Birth certificate.
- ✓ Proof of residence – i.e. Council tax or utility bill.
- ✓ Verification of full employment history for the past three years.
- ✓ Verification of nationality and immigration status.
- ✓ Verification of criminal record (unspent convictions only) through a third party agency such as Disclosure Scotland.

K.3.2.4 Where access is to systems processing payment card data, credit checks on the employee must be carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

K.3.2.5 All the above requirements for verification checks must be applied to technical support, contractors and temporary staff that have access to those systems or any copies of the contents of those systems (e.g. backup tapes, printouts, test data-sets) where there is not a contract with their employer or agency or the contract is deemed to give insufficient assurance.

K.3.2.6 By accepting their contract of employment that person is accepting that they understand the nature of the information they access, that they will not use the information for unauthorised purposes and that they will return or destroy any information or assets when their employment terminates.

K.3.3 Supplier's Remote Access to the Network

K.3.3.1 Partner agencies or 3rd party suppliers must not be given details of how to access the network without permission from ICT. Any changes to supplier's connections must be immediately sent to ICT so that access can be updated or ceased. All permissions and access methods must be controlled by ICT.

K.3.3.2 Partners or 3rd party suppliers must contact the IT helpdesk before connecting to the network and a log of activity must be maintained. Remote access software must be disabled when not in use.

K.3.4 Registering a new account

K.3.4.1 A request for access to the computer systems must first be submitted ICT team for approval. Applications must be made via the form on the intranet and it will require the approval of your line manager.

K.3.4.2 The person who is receiving the new account will be asked to sign a document saying they have received a copy of this document and where possible after an appropriate period (typically one month) will be asked to sign the document again to say they have read and understood the documents. This gives the opportunity to ask any questions, not just of the content of this document, but also ask general questions that may arise during the initial period of employment.

K.3.4.3 Decisions on the appropriate level of access to information or information systems for a particular individual are the responsibility of the System Owner.

K.3.5 Looking after your account

K.3.5.1 It is your responsibility to prevent your username and password being used to gain unauthorised access to corporate systems by:

- ✓ Choosing an appropriate password as described later in this section.

- ✓ Ensuring that any PC that is left unattended is locked or logged out.
- ✓ Leaving nothing on display that may contain access information such as login names and passwords.
- ✓ Informing the ICT team of any changes to roles and access requirements.

K.3.5.2 When an employee leaves the organisation, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the ICT team.

K.3.6 Choosing Passwords

K.3.6.1 Passwords are the first line of defence for our ICT systems and together with the username help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

K.3.6.2 A weak password is one that can be easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

K.3.6.3 A strong password is a password designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

K.3.6.4 Everyone must use strong passwords with a minimum standard of:

- At least seven characters.
- Contain at least three of the following five categories
- English uppercase characters (A - Z)
- English lowercase characters (a - z)
  - o Base ten digits (0 - 9)
  - o Non-alphanumeric (for example: !, $, # or %)
  - o Unicode characters

K.3.6.5 The Government advises using Environ passwords with the following format: consonant, vowel, consonant, consonant, vowel, consonant, number, number. An example for illustration purposes is provided below:

- Pinray4$

K.3.6.6 It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- ✓ Never reveal your passwords to anyone.
- ✓ Never use the 'remember password' function.
- ✓ Never write your passwords down or store them where they are open to theft.
- ✓ Never store your passwords in a computer system without encryption.
- ✓ Do not use any part of your username within the password.
- ✓ Where possible do not use the same password to access different systems.
- ✓ Do not use the same password for systems inside and outside of work.

K.3.6.7 All user-level passwords must be changed at a maximum of every **90** days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you must change it immediately and report your concern to the IT helpdesk. You must not reuse the same password within 24 password changes.

K.3.7 Application and Information Access

K.3.7.1 Access within software applications must be restricted using the security features built into the individual product. The system owner of the software application is responsible for granting access to the information within the system. The access must be:

- Compliant with the guidance given in this section
- Given the appropriate level of access required for the role of the person.
- Unable to be overridden (with the admin settings removed or hidden as appropriate).
- Free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Logged and auditable.

K.3.8 Changing roles and responsibilities

K.3.8.1 Line managers must notify the ICT helpdesk, in a timely manner, of any changes in a employee's role or business environment, to ensure that the access can be changed as appropriate.

K.3.9 Information Security Awareness, Education and Training

K.3.9.1 Everyone must receive appropriate information security awareness training and regular updates in related statute and organisational policies and procedures as relevant for their role where possible. It is the responsibility of Line managers to ensure that their staff are adequately trained and equipped to carry out their role efficiently and securely.

K.3.10 Closing accounts

K.3.10.1 Line managers must notify the ICT helpdesk in a timely manner of the impending termination or suspension of employment so that their access can be suspended. Line manager must ensure that all assets include any copies of information in any format are returned upon termination of their employment, contract or agreement.

K.3.10.2 ICT will notify the appropriate system owners who must suspend access for that individual at an appropriate time, taking into account the nature of the termination.

K.4 Routine operations

K.4.1 Definitions

K.4.1.1 We need to ensure the protection of the IT service (including any information systems and information processing equipment used by the business) against malware and malicious and mobile code and unscheduled outages, so the purpose of this section is to define the day-to-day processes.

K.4.1.2 Where the administration of the system has been devolved to a business unit, then an owner for the system will be identified and an agreement between that person and ICT will be established.

K.4.2 Documented Operating Procedures

K.4.2.1 We expect that there would be documented operating procedures for all of the key ICT systems both from a technical perspective to enable ICT to support the system and also at an appropriate level of detail for the departmental team that will be using them. It is the responsibility of the departmental team to create the business operations documents.

K.4.3 Change Management

K.4.3.1 Changes to the operational systems must be controlled through the change control procedure. Copies of the template for requesting changes is available from ICT. All changes need to be assessed for their impact on information security as part of the standard risk assessment.

K.4.4 Separation of Development, Test and Operational Facilities

K.4.4.1 Where possible, development and test environments must be separate from the live operational environment. This is in order to reduce the risk of accidental change or unauthorised access. The environments must be segregated by the most appropriate controls that are practical and ideally include, but not limited to, the following:

- Running on separate servers.

- Different usernames and passwords.

K.4.5 System Acceptance

K.4.5.1 All departments must inform the system owners via the IT Helpdesk of any new product requirements or of any upgrades, service packs, patches or fixes required to existing systems. All new products must be purchased through ICT.

K.4.5.2 New information systems, product upgrades, patches and fixes must all undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented and must involve system owners and management authorisation.

K.4.5.3 Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test environment that duplicates the operational system.

K.4.6 Protection against Malicious and Mobile Code

K.4.6.1 Appropriate steps are taken to protect the ICT systems, infrastructure and information against malicious code. Effective and up-to-date anti-virus software is run on all servers and PCs. Everyone is responsible for ensuring that they do not introduce malicious code into the ICT systems and this is described in the Removable Media section. Where a virus is detected on a corporate owned system, the individual must inform the IT Helpdesk.

K.4.6.2 Mobile code represents newer technologies often found in web pages and emails, and includes, but is not limited to:

- ActiveX.
- Java.
- JavaScript.
- VBScript.
- Macros.
- HTTPS.
- HTML.

K.4.7 Patching

K.4.7.1 All servers must have appropriate critical security patches applied in line with the corporate patching procedure. All other patches must be applied as appropriate. Patches must be applied to all software on the network where appropriate.

K.4.8 Information Backup

K.4.8.1 Regular backups of essential business information held on the servers are taken to ensure that the it is possible to recover from a disaster, media failure or error. An appropriate backup cycle must be used and fully documented.

K.4.8.2 Any 3rd parties that store the organisation's information must also be required to ensure that the information is backed up.

K.4.8.3 Removable media must not be used as the only method of storage as it is not backed up, please see the section on removable media for more information.

K.4.9 Storage Media Handling

K.4.9.1 Storage media includes, but is not restricted, to the following:

- Computer Hard Drives (both internal and external).
- CDs.
- DVDs.
- Optical Disks
- USB Memory Sticks
- Media Card Readers.
- MP3 Players.
- Digital Cameras.

- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).
- Other emerging technologies such as cloud storage.

K.4.10 Physical Storage Media in Transit

K.4.10.1 Storage media being transported must be protected from unauthorised access, misuse or corruption. Where couriers are required a list of reliable and trusted couriers must be established. If appropriate, physical controls such as encryption or special locked containers must also be used.

K.4.10.2 For further information, please refer to the Removable Media section.

K.4.11 Disposal of Storage Media

K.4.11.1 Storage media that is no longer required must be disposed of safely and securely to avoid data leakage.

K.4.11.2 Any previous contents of any reusable storage media that are to be removed from the organisation must be erased. This must be a thorough removal of all data from the storage media to avoid the potential of data leakage.

K.4.11.3 For further information, please refer to the Removable Media section.

K.4.12 Security of System Documentation

K.4.12.1 System documentation must be protected from unauthorised access. This includes bespoke documentation that has been created by the information services provider or any other departmental IT staff. This does not include generic manuals that have been supplied with software). Examples of the documentation to be protected include, but are not restricted to, descriptions of:

- Applications.
- Processes.
- Procedures.
- Data structures.
- Authorisation details.

K.4.12.2 Effective version control must be applied to all documentation and documentation storage.

K.4.13 Clock Synchronisation

K.4.13.1 All computer clocks are synchronised to a central time source to ensure the accuracy of all the systems audit logs as they may be needed for incident investigation. You must not change the time on any computer or device.

K.4.14 Wireless Networks

K.4.14.1 Wireless networks present their own set of challenges particularly when connecting to public wireless networks in venues such as coffee shops. Care must be taken when connecting to these networks that they are reputable and you must not access any PSN or OFFICIAL material while connecting to them.

K.4.15 Protection of System Test Data

K.4.15.1 If personal information is used during the development and test phase of preparing application software it must be protected and controlled in line with the Data Protection Act and where possible depersonalised. If operational data is used controls must be used including, but not limited to, the following:

- An authorisation process.
- Removal of all operational data from the test system after use.
- Full audit trail of related activities.
- Any personal or confidential information must be protected as if it were live data.

K.4.16 Annual Health Check

K.4.16.1 An annual health check of all IT infrastructure systems and facilities is undertaken by ICT every 12 months. This health check includes, but is not restricted to, the following:

- An attempt to break into the network from outside.
- A network summary that will identify all IP addressable devices.
- Network analysis, including exploitable switches and gateways.
- Vulnerability analysis, including patch levels, poor passwords and services used.
- Exploitation analysis.
- A summary report with recommendations for improvement.

K.4.17 Modems

K.4.17.1 The use of modems connected to the ICT network can potentially seriously compromise the security of the network. The normal operation of the network must not be interfered with and specific approval must be obtained from the ICT team before connecting any equipment to the network.

K.5 Computer, Telephone and Desk Usage

K.5.1 Definition

K.5.1.1 The organisation handles large amounts of sensitive information. The security of this information is of paramount importance. Ensuring a clear desk approach can help prevent the security of this information from being breached.

K.5.1.2 The purpose of this section is to establish guidelines as to what constitutes “computer and telephony resources”, what is considered to be “misuse” and how you would ideally operate within a clear desk environment.

K.5.1.3 Computer and telephony resources currently available include, but are not restricted to, the following:

- Mainframe computers.
- Departmental computers.
- Personal computers.
- Portable laptop computers.
- Terminals.
- Printers.
- Network equipment.
- Telecommunications facilities.
- Other emerging technologies such as tablets and wearable computers.

K.5.2 Computer Resources Misuse

K.5.2.1 No exhaustive list can be prepared defining all possible forms of misuse of computer resources. The individual circumstances of each case will need to be taken into account. However, some examples are outlined below:

- Use of computer resources for the purposes of fraud, theft or dishonesty.
- Storing/loading/executing of software for a purpose that is not work related.
- Storing/loading/executing of software that:
  - Has not been acquired through approved procurement procedures.
  - The organisation does not hold a valid program licence.
  - Has not been the subject of formal virus checking procedures.
- Storing/processing/printing of data for a purpose that is not work related.

K.5.3 Telephone

K.5.3.1 We have an Acceptable Use Procedure / Code of Practice relating to telephone use. This relates to the use of static and mobile telephones for private telephone calls. This is at the end of this section and must be adhered to at all times. The purchase of telephones must be agreed with ICT so there is a complete record of the phones in use across the organisation and that the organisation's purchasing power is maximised. The criteria for allocating a device will be at the line manager's discretion and the range of devices available will be limited to those supported by the organisation and appropriate for the working conditions. It is expected that you will ensure you are aware of any procedures relating to the use of phones, particularly in relation to health and safety and using the telephone while driving. If you need further information you must contact Health and Safety. If your phone develops any faults or is damaged you must contact ICT who can assist in repair or replacement. If the phone is allocated to a group of people then it is the responsibility of the manager to ensure that the phone is properly managed and any costs are appropriately allocated.

K.5.4 Clear Desk

K.5.4.1 We recommend a clear desk in order to ensure that all information is held securely at all times. Wherever possible work must not be left on desks unattended and must be removed from view when unsupervised. At the end of each day, every desk must be cleared of all documents that contain any sensitive information, or any information relating to clients or citizens.

K.5.4.2 Unclassified material, together with non- business related specific operating manuals may be left in an ordered manner on desks. Work must ideally be stored in a locked cupboard overnight, and there must be nothing left on desks at the end of the working day. Trays containing work must be locked away in cabinets or drawers.

K.5.4.3 All information classified as OFFICIAL must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level. Nothing must be left lying on printers, photocopiers or fax machines at the end of the day.

K.5.4.4 It is your responsibility for safeguarding data by ensuring that equipment is not left logged-on when unattended, and that portable equipment is not exposed to opportunistic theft. Computer equipment is equipped with facilities to lock automatically and you must not tamper with this security feature. You must not change any lock settings on mobile data devices such as Blackberry's and laptops.

K.5.4.5 Remember, when you are not working at your workstation there could be a business requirement for other staff to use that station.

K.5.4.6 Floor space under furniture and around the office needs to remain free from obstructions at all times to facilitate the cleaning and maintenance of the building. Departmental Managers may choose to undertake checks of their area and any items that are found on the floor (apart from footrests and bins) removed. As part of good housekeeping, boxes, folders etc. must not be stored on top of furniture, cabinets, window ledges etc.

K.5.4.7 A clear desk approach is not intended to hinder your day to day working. In an ideal world, we would all work with a clear desk.

K.5.5 Personal Telephone Calls

K.5.5.1 Employees may need to make calls (this includes sending text messages or accessing websites) of a personal nature while at work. We expect you to ensure that the provision of your service is not compromised and there is no financial loss.

K.5.5.2 Wherever possible, private calls must be made outside of the standard hours of service provision, i.e. before 9pm, after 5pm, or during a lunch break. The calls must be kept to a minimum, so as not to prevent business calls getting through. If you are using a static phone you must keep a record of the private calls and contact the Cashiers to allow the cost to be recovered. Where an itemised telephone bill is available, the actual cost of each private call per the bill (plus VAT) will be recharged to the relevant employee. Employees can request the details of the itemised bills to check against their own records of private calls. Where itemised bills are not available, please contact the Cashiers for the appropriate rates.

K.5.5.3 If you have an organisation provided mobile phone then it is your responsibility to ensure that the list of your personal numbers held by ICT is accurate and up to date. This information is used to automatically calculate the monthly cost of personal calls that are recharged to you.

K.5.5.4 Where private calls from a mobile telephone are made but are not charged on the bill because they form part of a free use period within the contract, the employee will calculate the cost of the call at the normal tariff for the day and time that the call was made and pay that amount.

K.6 Email usage

K.6.1 Definition

K.6.1.1 The purpose of this section is to establish a framework so that employees can apply self-regulation to their use of email as a communication and recording tool.

K.6.1.2 All email prepared and sent from corporate email addresses or mailboxes, and any non-work email sent using the ICT facilities is subject to this section.

K.6.2 Email as Records

K.6.2.1 All emails that are used to conduct or support official business must be sent using a corporate email address. All emails sent via the Public Sector Network must have a Public Sector Network email access.

K.6.2.2 Non-work email accounts must not be used to conduct or support official business. It is each person's responsibility to ensure that any emails containing sensitive information must be sent from an official email address. Any emails containing OFFICIAL information must be sent from a PSN email address. All emails that represent aspects of the organisation's business or administrative arrangements are the property of the business and not of any individual employee.

K.6.2.3 Emails held on corporate equipment are considered to be part of the corporate record and email also provides a record of staff activities.

K.6.2.4 The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official business must be considered to be an official communication from the business.

K.6.2.5 While respecting the privacy of those authorised to use the IT systems or networks, the organisation maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised people to ensure adherence to this section. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. You must be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the ICT systems.

K.6.2.6 Also it needs to be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the Legal section.

K.6.3 Email as a Form of Communication

K.6.3.1 Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or OFFICIAL information or of communicating in the particular circumstances.

K.6.3.2 Email must not be considered to be any less formal than memos or letters that are sent out from a particular service or the authority. When sending external email, care must be taken not to contain any material that would reflect poorly on the organisation's reputation or its relationship with customers, clients or business partners.

K.6.3.3 Under no circumstances must you communicate material (either internally or externally), that is, for example, defamatory, obscene, or does not comply with the organisation's Equal Opportunities Procedure, or that could reasonably be anticipated to be considered inappropriate. Anyone who is unclear about the appropriateness of any material must consult their line manager prior to commencing any associated activity or process. Email facilities must not be used for:

- Activities that:
  - Corrupt or destroy other peoples' data.
  - Disrupt the work of others.
  - Unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to others.
  - Violate the privacy of others.
- Jargon, abbreviations or symbols if these might not be readily understood by the recipient.
- Publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- Replacing face-to-face discussion where face-to-face is more appropriate.
- So-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms.
- The creation or transmission of:
  - Anonymous messages - i.e. without clear identification of the sender.
  - Any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
  - Defamatory material.
  - Material that infringes the copyright of another person, including intellectual property rights.
  - Material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
  - Material that includes false claims of a deceptive nature.
  - Material that brings the organisation into disrepute.
  - Material that is designed or likely to cause annoyance, inconvenience or needless anxiety or that is abusive or threatening to others, or serves to harass or bully others.
  - Unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- The sending of messages in capitals – it is the equivalent of shouting at someone.
- Unfairly criticising individuals, including copy distribution to other individuals.
- Wasting resources by printing out messages received unless a hard copy is essential.

K.6.4 Junk Mail

K.6.4.1 There may be instances where you will receive unsolicited mass junk email or spam. It is advised that you delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

K.6.4.2 Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

K.6.4.3 Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) must not be forwarded using ICT systems or facilities.

K.6.5 Mail Box Size

K.6.5.1 In order to ensure that the systems enabling email are available and perform to their optimum, you must endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of e-mail addresses is discouraged.

K.6.5.2 You are provided with a limited mail box size to reduce problems associated with server capacity. Everyone with email access must manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems.

K.6.5.3 Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists must be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox.

K.6.6 Categorisation of Messages

K.6.6.1 When creating an email and where tools have been implemented, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. For further information on the classifications available please see the section on Information Protection.

K.6.7 Confidentiality

K.6.7.1 Everyone is under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If you are unsure if you can pass on information, you must contact the Data Protection Officer.

K.6.7.2 Staff must make every effort to ensure that confidentiality is appropriately maintained. Staff must be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent outside the organisation, because of the insecure nature of such networks and the number of people to whom the messages can be freely circulated without the knowledge of the business.

K.6.7.3 Care must be taken when addressing all emails, but particularly where they include OFFICIAL information, to prevent accidental transmission to unintended recipients. Particular care needs to be taken if the email client software auto-completes an email address as you begin typing a name.

K.6.7.4 Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent OFFICIAL material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the IT helpdesk in the first instance.

K.6.7.5 The automatic forwarding of email from the Public Sector Network to lower classified email addresses (i.e. a standard .gov.uk email) outside of the organisation contradicts national guidelines and is not acceptable.

K.6.8 Negligent Virus Transmission

K.6.8.1 Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of anti-virus software. If anyone has concerns about possible virus transmission, they must report the concern to the ICT helpdesk. In particular, you must:

- ✓ Ensure that an effective anti-virus system is operating on any computer that you use to access corporate facilities.
- ✓ Not download data or programs of any nature from unknown sources.
- ✓ Not forward virus warnings other than to the IT helpdesk.
- ✓ Not transmit by email any file attachments that you know to be infected with a virus.
- ✓ Report any suspected files to the IT helpdesk.

K.6.8.2 If a computer virus is transmitted to another organisation, the organisation could be held liable if there has been negligence in allowing the virus to be transmitted.

K.7 Information Security Incident Management

K.7.1 Definition

K.7.1.1 The definition of an Information Security Incident is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

K.7.1.2 An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the organisation's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

K.7.1.3 Examples of some of the more common forms of Information Security Incidents are;

- Malicious
  - Giving information to someone who is not entitled to have access to it - verbally, in writing or electronically.
  - Computer infected by a Virus or other malware.
  - Sending a sensitive e-mail to 'all staff' by mistake.
  - Receiving unsolicited mail of an offensive nature.
  - Receiving unsolicited mail that requires you to enter personal data.
  - Finding data that has been changed by an unauthorised person.
  - Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails that encourage you to forward onto others.
  - Unknown people asking for information that could gain them access to corporate data (e.g. a password or details of a third party).
- Misuse
  - Use of unapproved or unlicensed software on corporate equipment.
  - Accessing a computer database using someone else's authorisation (e.g. someone else's username and password).
  - Writing down your password and leaving it on display / somewhere easy to find.
  - Printing or copying confidential information and not storing it correctly or confidentially.
  - Not sending protectively by marked documents via the appropriate channel
- Theft / Loss
  - Theft / loss of a hard copy file.
  - Theft / loss of any computer equipment.

K.7.2 Procedure for Incident Handling

K.7.2.1 Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the ICT team. This enables the ICT team to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the ICT team to gain as much information as possible to identify if an incident is occurring.

K.7.2.2 Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. Everyone must understand, and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected you must:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from ICT).
- Not use any removable media (for example USB memory sticks) that may also have been infected.

K.7.2.3 If the Information Security incident is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to Senior Management and the Data Protection Officer for the impact to be assessed.

K.7.2.4 The IT Helpdesk will require you to supply further information depending upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

K.7.2.5 Security weaknesses, for example a software malfunction, must be reported through the same process as security events. You must not attempt to prove a security weakness as such an action may be considered to be misuse. Weaknesses reported to application and service providers by employees must also be reported internally to ICT.

K.7.3 Management of Information Security Incidents and Improvements

K.7.3.1 A consistent approach to dealing with all security events must be maintained across the organisation. The events must be analysed and the ICT team must be consulted to establish when security events become escalated to an incident.

K.7.3.2 All high and medium incidents must be reported to the IT helpdesk and the onsite ICT team. All low incidents must be reported to the IT helpdesk. To decide what level of impact an incident has employees must refer to the Risk Impact Matrix at the end of this section.

K.7.4 Collection of Evidence

K.7.4.1 If an incident may require information to be collected for an investigation strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation, for example concerning computer misuse, contact the ICT team for advice.

K.7.5 Learning from Information Security Incidents

K.7.5.1 To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.

- Costs incurred during the incidents.

K.7.5.2 The information must be collated and reviewed on a regular basis by ICT team and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.

K.7.5.3 The information, where appropriate, must be shared with the Warning, Advice and Reporting Point (WARP) to aid the alert process for the region.

K.7.6 Risk Impact Matrix

K.7.6.1 To decide on the potential or actual impact of an information security incident, the impact matrix below must be used.

Type of Impact	Reputational Media and Senior Management Damages	Reputational Loss within Government and / or Failure to Meet Statutory / Regulatory Obligations	Contractual Loss	Failure to meet Legal Obligations	Financial Loss / Commercial Confidentiality Loss	Disruption to Activities	Personal Privacy Infringement
High	Unfavorable media interest	External investigation with the potential for sanctions or financial loss	Failure to retain contract(s) at the point of renewal	Civil lawsuit / small fine - less than £10,000.	Any financial loss	Any disruption to service greater than one working day	Personal details revealed or compromised externally or harm to the mental or physical wellbeing of any employee or public
Medium	Unfavorable senior management response	Internal investigation or disciplinary involving one individual	Significant client dissatisfaction. Major SLA failures. Failure to attract new business	None	None	Minor disruption to service activities that can be recovered	Personal details revealed or compromised within organisation
Low	Contained internally within the organisation	None	Minor contractual problems / minimal SLA failures	None	None	Minor disruption to service activities that can be recovered	None

K.8 Internet Usage

K.8.1 Definition

K.8.1.1 This section tells you how you must use the Internet access. It outlines your personal responsibilities and informs what you must and must not do. Internet access is made available for the business purposes of the organisation. A certain amount of personal use is permitted in accordance with the statements contained within this section.

K.8.1.2 It is recognised that it is impossible to define precise rules covering all Internet activities available and adherence must be undertaken within the spirit of the policy to ensure productive use of the facility is made. This document updates the Internet and email procedure and replaces all locally agreed Internet usage policies.

K.8.2 Using the internet

K.8.2.1 The Internet access is primarily provided to give:

- Access to information that is pertinent to fulfilling the business obligations.
- Supporting business applications that are run over the internet.

- The capability to post updates to the organisation's owned and/or maintained web sites.
- An electronic commerce facility.

K.8.3 Personal Use of the Internet Service

K.8.3.1 At the discretion of your line manager, and provided it does not interfere with your work, you can use of the Internet in your own time (for example during your lunch-break).

K.8.3.2 We are not; however, responsible for any personal transactions you enter into - for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep the organisation protected against, any claims, damages, losses or the like that might arise from your transaction - for example in relation to payment for the items or any personal injury or damage to property they might cause.

K.8.3.3 If you purchase personal goods or services via the Internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the organisation unless approved by ICT or your line manager. You must ensure that personal goods and services purchased are not delivered to the business premises. Rather, they must be delivered to your home or other personal address.

K.8.4 Internet filtering

K.8.4.1 The organisation has a filter in place to prevent access to various categories of sites that are in principle not within the spirit of the internet access. The categories below are those that are blocked as standard, however it is accepted that there may be a business need to access sites inside these categories and you must talk to ICT (or use the form that appears when accessing a site) about either changing the classification or allowing permanent access to one of these categories:

- Adult/Sexually Explicit
- Advertisements & Pop-Ups
- Alcohol & Tobacco
- Criminal Activity
- Gambling
- Hacking
- Illegal Drugs
- Intolerance & Hate
- Phishing & Fraud
- Proxies & Translators
- Spam URLs
- Spyware
- Streaming Media
- Tasteless & Offensive
- Violence
- Weapons

K.8.5 Internet Monitoring

K.8.5.1 All internet access is recorded, logged and interrogated for the purposes of:

K.8.5.2 Monitoring total usage to ensure business use is not impacted by lack of capacity.

K.8.5.3 The filtering system monitors and records all access for reports that are produced for line managers and auditors.

K.8.5.4 There is an internet monitoring group comprising of ICT, Audit and Personnel who review the usage of anyone who exceeds twenty hours of usage in any one calendar month to ensure they are remaining within the spirit of this section.

K.8.6 Things You Must Not Do

K.8.6.1 Except where it is strictly and necessarily required for your work, you must not use your Internet account to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter “money making” sites or enter or use “money making” programs.
- Run a private business.
- Download any software that does not comply with the section on software.

K.8.6.2 The above list gives examples of “unsuitable” usage but is neither exclusive nor exhaustive. “Unsuitable” material would include data, images, audio files or video files that is illegal to transmit under British law, and, material that is against the rules, essence and spirit of this and other policies.

K.8.7 Your Responsibilities

K.8.7.1 This section relies on employees acting responsibly and in accordance with the above rules. Where employees have concerns that colleagues are acting in breach of the above rules, they are encouraged to raise these concerns under the Whistleblowing procedure.

K.8.8 Line Manager’s Responsibilities

K.8.8.1 It is the responsibility of Line Managers to ensure that the use of the Internet facility:

- Within an employees work time is relevant to and appropriate to the business and within the context of the employees responsibilities.
- Within an employee’s own time is subject to the rules contained within this document.
- Where usage reports are provided these are reviewed on a regular basis.

K.9 ICT Infrastructure

K.9.1 Definition

K.9.1.1 This section defines how paper and electronic information belonging to the organisation must be protected and, offers guidance on how such protection can be achieved. It also describes employee roles and the contribution staff make to the safe and secure use of information.

K.9.2 Secure Areas

K.9.2.1 OFFICIAL information must be stored securely. A risk assessment must identify the appropriate level of protection to be implemented to secure the information being stored.

K.9.2.2 Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have appropriate control mechanisms in place for the type of information and equipment that is stored there.

K.9.2.3 As an example, access to secure areas such as the data centre and ICT equipment rooms must be adequately controlled and physical access to buildings needs to be restricted to authorised persons. Staff working in secure areas must challenge anyone not wearing a badge.

K.9.2.4 Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and must not be loaned/provided to anyone else.

K.9.2.5 Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. An employee from ICT must monitor all visitors accessing secure IT areas at all times.

K.9.2.6 Keys to all secure areas housing ICT equipment and lockable ICT cabinets are held centrally by ICT, as appropriate. Keys are not stored near these secure areas or lockable cabinets.

K.9.2.7 In all cases where security processes are in place, instructions must be issued to address the event of a security breach. Where breaches do occur, or an employee leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) must be recovered from the employee and any door/access codes needs to be changed immediately. Please also refer to the IT Access section.

K.9.3 Non-Electronic Information Security

K.9.3.1 Paper based (or similar non-electronic) information must be assigned an owner and a classification as stated in Information Protection section. If it is classified as OFFICIAL information security controls to protect it must be put in place. A risk assessment must identify the appropriate level of protection for the information being stored. Paper in an open office must be protected by the controls for the building and via appropriate measures that could include, but are not restricted to, the following:

- Filing cabinets that are locked with the keys stored away from the cabinet.
- Locked safes.
- Stored in a Secure Area protected by access controls.

K.9.4 Equipment Security

K.9.4.1 All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g. if necessary items such as laptops must be physically attached to the desk.
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

K.9.4.2 Desktop PCs must not have data stored on the local hard drive. Data must be stored on the network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

K.9.4.3 All servers located outside of the server room must be sited in a physically secure environment. Business critical systems must be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from ICT.

K.9.4.4 All items of equipment are recorded on the ICT inventory and procedures are in place to ensure it is updated as soon as assets are received or disposed of. All equipment must be security marked and have a unique asset number allocated to it. You must not remove or deface any asset registration number.

K.9.4.5 For portable computer devices please refer to the Remote Working section.

K.9.5 Cabling Security

K.9.5.1 Cables that carry data or support key information services must be protected from interception or damage. Power cables must be separated from network cables to prevent interference. Network cables must be protected by conduit and where possible avoid routes through public areas.

K.9.6 Secure Disposal or Re-use of Equipment

K.9.6.1 Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools and returned to ICT for disposal.

K.9.6.2 Software media or services must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

K.9.7 Regular Audit

K.9.7.1 There is a duty to audit information security arrangements regularly to provide an independent appraisal and recommend security improvements where necessary.

K.10 Remote Working

K.10.1 Definition

K.10.1.1 The mobility, technology and information that make portable computing devices so useful to employees and organisations also make them valuable prizes for thieves. Securing OFFICIAL data when you work remotely or beyond the organisation's network is a pressing issue – particularly in relation to the need to protect data in line with the requirements of the Data Protection Act 1998.

K.10.1.2 Portable computer devices include, but are not restricted to, the following:

- Laptop computers.
- Tablet PCs.
- PDAs.
- Palm pilots.
- Mobile phones.
- Text pagers.
- Wireless technologies.

K.10.2 Remote and Mobile Working Arrangements

K.10.2.1 All IT equipment (including portable computer devices) supplied by the organisation is the property of the organisation. It must be returned upon the request and you must allow access for ICT to perform maintenance and audit tasks. You must not remove or deface any asset registration number.

K.10.2.2 Remote workers must ensure that their portable computer devices are connected to the corporate network at least once every two weeks to enable the anti-virus software to be updated.

K.10.2.3 You need to be aware of the physical security dangers and risks associated with working within any remote office or mobile working location and when moving between home and another business site. Equipment must not be left where it would attract the interests of the opportunist thief. In the home it must also be located out of sight of the casual visitor. For home working it is recommended that the office area of the house needs to be kept separate from the rest of the house. Equipment must be secured whenever it is not in use. When using your computer you must be aware of people around you to avoid the accidental or deliberate overlooking by unauthorised individuals, who may see personal or business information they are not entitled to see.

K.10.2.4 Business critical data must be stored on a file and print server wherever possible and not held on the portable computer device and under no circumstances must Personal or OFFICIAL information be emailed to a private non-corporate email address. For further information, please refer to the section on email usage.

K.10.2.5 You must ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times. All removable media devices and paper documentation must also not be stored with the portable computer device.

K.10.2.6 Where you access Public Sector Network type services, under no circumstances must non-corporately owned equipment be used.

K.10.2.7 Paper documents are vulnerable to theft if left accessible to unauthorised people. These must be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents must be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing OFFICIAL information must be returned to the office and shredded.

K.10.2.9 If you are planning to take corporately owned equipment outside the United Kingdom you must seek advice. The equipment may not be covered by the normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel.

K.10.2.10 The IT equipment can be used for personal use so long as it is not used in relation to an external business. Only software supplied and approved can be used (e.g. Word, Excel, Adobe, etc.). No family members may use the IT equipment. The IT equipment is supplied for your sole use.

K.10.3 Access Controls

K.10.3.1 It is essential that access to all OFFICIAL information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls.

K.10.3.2 Portable computer devices must be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

K.10.3.3 All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all OFFICIAL data held on the portable computer device must be encrypted.

K.11 Removable Media

K.11.1 Definition

K.11.1.1 There are risks associated with accessing and handling information in order to conduct official business. Information is used throughout the business and sometimes shared with external organisations and applicants. Securing OFFICIAL data is of paramount importance – particularly in relation to the need to protect data in line with the requirements of the Data Protection Act 1998. Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the organisation.

K.11.1.2 Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

K.11.2 Restricted Access to Removable Media

K.11.2.1 Removable media must be treated with the same care as other controlled stationery such as cheque books. The use of removable media devices will only be approved if a valid business case for its use is developed. Requests for access to, and use of, removable media devices must be made to ICT. If access to, and use of, removable media devices is approved the following sections apply and must be adhered to at all times.

K.11.3 Procurement of Removable Media

K.11.3.1 All removable media devices and any associated equipment and software must only be purchased and installed by ICT. Non-corporately owned removable media devices must not be used to store any information used to conduct official business, and must not be used with any corporately owned or leased IT equipment.

K.11.4 Security of Data

K.11.4.1 Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data that is frequently backed up. Therefore removable media must not be the only place where data obtained for business purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system. For further information please see the sections on Remote Working and Communications and Operation Management.

K.11.4.2 In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment. Damaged or faulty removable media devices must not be used and you must contact the IT helpdesk if the removable media device be damaged.

K.11.4.3 Everyone who has a removable media device is responsible for the appropriate use and security of data and for not allowing the information stored on these devices, to be compromised in any way whist in their care or under their control.

K.11.4.4 While in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the organisation, other organisations or individuals from the data being lost while in transit or storage.

K.11.4.5 All data stored on removable media devices must be encrypted. If this is not possible, then all OFFICIAL data held must be encrypted.

K.11.4.6 Virus and malware checking software approved by ICT must be operational on both the machine the data is taken and the machine where the data is to be loaded.

K.11.4.7 You must be aware that ICT will audit / log the transfer of data files to and from all removable media devices and corporately-owned IT equipment.

K.11.5 Incident Management

K.11.5.1 It is your duty to immediately report any actual or suspected breaches in information security in accordance with the process in the Information Security Incident Management section.

K.11.5.2 Any misuse or irresponsible actions that affect business data, or any loss of data, must be reported as a security incident to the IT helpdesk.

K.11.6 Third Party Access to Information

K.11.6.1 No third party (external contractors, partners, agents, public or non-employee parties) may receive data or extract information from the ICT network, information stores or IT equipment without explicit agreement from ICT. If third parties are allowed access to information then all the considerations of this section apply to their storing and transferring of the data.

K.11.7 Disposing of Removable Media Devices

K.11.7.1 All removable media devices that are no longer required, or have become damaged, must be returned to ICT for secure disposal. Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused must be erased.

K.12 Social media Usage

K.12.1 Definition

K.12.1.1 Social media is an emerging channel of communication that runs in tandem with traditional forms. It includes sites like Facebook, Twitter and more.

K.12.1.2 The communications team has been using social media since early 2009, with a good deal of success and a number of very positive case studies that show this can be a good method for resident and customer engagement when used wisely.

K.12.2 Corporate social media accounts

K.12.2.1 There are corporate Facebook, Flickr, Twitter and Youtube accounts that are managed by the communications team in line with PR protocols. All press releases and press photographs are automatically posted to these sites as appropriate.

K.12.2.2 If you want to add tweet or a post to any of these accounts, please contact the communications team and they can talk you through the process.

K.12.3 Setting up your service social media sites, accounts and more

K.12.3.1 You may wish to set up a social media channel, such as Twitter, YouTube, Facebook, blogs on behalf of your service area. If you are considering this, you must first seek the approval of your line manager and director. Please note: If you do not get approval you may not set up an account on behalf of the organisation/your service.

K.12.3.2 When approved, you must book in a session with the communications team before you set the account up. The session will cover:

- How quickly you will respond to posts through these channels.
- How to approve posts and responses to negative issues.
- How to resource the activity (if it is just one officer, who will deputise when you are away from work?).
- The reasons for using the channel.
- What you can and cannot say.
- Your experience of using social media networks.
- If you set up a blog, you need to be aware that you may find yourself responding to comments on your blog. One blog received on average ten comments on each news item posted, this required a considerable amount of work for the team responding to these questions and resulting questions.

K.12.3.3 As a golden rule – it is worth remembering that while it is very easy to set up social media accounts, it is time intensive to use and manage them properly and you need to be geared up to add this activity to your existing workload.

K.12.4 Being social media active as an employee

K.12.4.1 As an employee, you may have your own personal accounts on things like Twitter and Facebook, and you may be 'friends' with or 'following' the organisation's social media feeds via your own account.

K.12.4.2 When it comes to commenting on posts or tweets, please feel free to post positive comments 'I really enjoyed last night's event' for example, but do not post negative comments or engage in any negative discussions online. This is because as an employee you are also a representative of the organisation. As such your response could be considered 'the organisation's position' and, as with all other responses to negative issues, the response needs to be checked first, through established PR protocols, to make sure it is balanced and accurate. This applies whether you are posting during work time or at home in your own time.

K.12.4.3 When commenting in your official role, on an official corporate site, or on the corporate accounts:

- Do not disclose confidential information, make comments, commitments or engage in activities on behalf of the organisation, unless you are authorised to do so.
- If you have any doubts, take advice from your line manager or contact the communications team.
- Always remember that online interaction results in your comments being permanently available and open to being republished in other media.

- Stay within the legal framework and be aware that libel, defamation, copyright and data protection laws apply.
- Be aware that engaging in social media may attract media interest in you as an individual, so proceed with care whether you are participating in either an official or a personal capacity.

K.12.4.4 When engaging in social media as an individual we would recommend that you:

- Always remember that online interaction results in your comments being permanently available and open to being republished in other media.
- Be aware that engaging in social media may attract media interest in you as an individual, so proceed with care whether you are participating in either an official or a personal capacity.
- Stay within the legal framework and be aware that libel, defamation, copyright and data protection laws apply.
- Remember that joining any controversial online single-issue groups or forums, even if you are doing it in your leisure time, could reflect badly on you as an employee. Please refer to our Equality & Diversity policy.

K.12.5 Five golden rules for social media

- Be credible, accurate, fair, thorough and transparent.
- Be consistent, cordial, honest and professional at all times.
- Be responsive, social media is like a public discussion forum. Respond as soon as you can, otherwise it will reflect badly on the service/organisation if you leave a question unanswered for a long period of time.
- Be integrated - Wherever possible align online participation with other offline communications (press releases, leaflets etc.).
- Be a responsible officer Remember that you are an ambassador for the organisation and the code of conduct still applies in your leisure time.

K.12.6 Contact us

K.12.6.1 Please forward any negative issues on the social media accounts to the communications team who will deal with it in line with corporate protocols.

K.12.6.2 If you have any questions relating to social media contact the communications team.

K.13 Software

K.13.1 Software Acquisition

K.13.1.1 Software is an asset and must be purchased through ICT. Software may not be purchased through corporate credit cards, petty cash, travel or entertainment budgets unless agreed with ICT. This so there is a record of all software purchased and we can register, support, and upgrade the software accordingly. This includes software downloaded and/or purchased from the Internet. If you want a new piece of software you must discuss it with ICT before purchasing as there may be software available that meets your needs.

K.13.1.2 Under no circumstances must personal or unsolicited software (this includes screen savers, games and wallpapers etc.) be loaded onto a corporately owned machine as there is a serious risk of introducing a virus and/or breaching the licensing conditions associated with that piece of software.

K.13.2 Software Registration

K.13.2.1 We use software in all aspects of our business to support the work we do. In all instances every piece of software is required to have a licence (even if it a freeware licence) and we will not condone the use of any software that does not have a licence. ICT use a software asset management tool to maintain a register of all software titles and their associated licenses.

K.13.2.2 The software must be registered in the official name of the organisation. Due to personnel turnover, software must never be registered in an individual's name.

K.13.2.3 Unless it is authorised by the software manufacturer, copying software is an offence under the Copyright, Designs and Patents Act 1988. We do not condone illegal duplication of software and will not tolerate it.

K.13.3 Software Installation

K.13.3.1 We have controls in place to prevent the installation of software, however some packages will try to circumvent these, therefore software must only be installed by ICT. Once installed, the original media or downloaded files will be kept in a safe storage area maintained by ICT.

K.13.3.2 Shareware, Freeware and Public Domain Software are bound by the same policy as all other software. You must not install any free or evaluation software without prior approval from ICT. Software cannot be taken home and loaded on a home computer without first discussing with ICT to ensure licence conditions are met. You must not bring software from home (or any other external source) and load it onto the computers.

K.13.4 Software Development

K.13.4.1 Software must not be changed or altered unless there is a clear business need. All changes must be authorised before the change is implemented. The change control procedure that needs to be adhered to is detailed elsewhere in this policy.

K.13.5 Software Disposal

K.13.5.1 All software packages are the property of the organisation whether they are purchased by an individual department or ICT. When you no longer need a piece of software you must tell ICT so it can be uninstalled and made available for others to use. In addition the software asset management tool ICT operate can identify where software is not being used and the licences will be taken back into the central pool.

K.13.6 Software Misuse

K.13.6.1 ICT will ensure that Personal Firewalls are installed where appropriate and you must not attempt to disable or reconfigure the Personal Firewall software. It is everyone's responsibility to report any known software misuse to ICT.