School ICT Infrastructure Requirements for Teaching Computing

A Computing at School (CAS) Whitepaper

By Brian Lockwood and Richard Cornell

September 2013

COMPUTING AT SCHOOL

EDUCATE · ENGAGE · ENCOURAGE

In collaboration with BCS, The Chartered Institute for IT

Table of Contents

1 Executive Summary

School ICT Infrastructure and how it is managed can be one the biggest impediments in the implementation of Computer Science education. The needs of teachers and learners and the requirements imposed on network managers, whether in-house or outsourced, can be a source of conflict. The sometimes apparently diametrically opposing position of the service provider and their end users has always been there and it applies to the teaching of other subjects not just Computer Science or ICT.

The introduction of Computer Science as an academic subject adds a further layer of complication to the challenging landscape of school IT infrastructure. Without the right support and information, school IT infrastructure cannot deliver the processing power and networking facilities that students need for computer science without compromising security or integrity of the other users on the system or their data.

With good training and management, in-house and third party service providers can support the specialist needs of all teachers. This will mean that teachers do not have to struggle with a system that is heavily tied down because the necessary protections are implemented correctly and they function quietly in the background.

The experience from many CAS members has shown that it is possible to teach Computer Science with support from senior leadership, a constructive dialog with the service provider and the cooperation from a student body supported by a well understood Acceptable Use Policy.

There are a range of technical solutions available to facilitate the teaching and learning of Computer Science which can accommodate all budgets and support provider skill levels. Many of these will fit easily into existing support arrangements or contracts without jeopardising SLAs or the integrity of the whole-school ICT system. Together with a senior management led Computer Science strategy, a mechanism for implementing solutions and a good change management process success can be achieved.

When a school decides to enter into an outsourcing agreement or decides to renegotiate with their internal support team they need to make sure the needs of the teachers and learners of Computer Science are considered. A balance can be struck between these groups if the following are considered and accounted for in any contracts or agreements:

- Computer Science teachers, more so than other subject teachers, need specialist ICT tools;
- Learners need access to specialist ICT tools and need to investigate and understand how operating systems work;
- The teaching and learning of Computer Science requires experimentation and creative problem solving which may necessitate new ICT tools that were not defined in advance;
- A change management process needs to be able to cope with the demands of teachers and learners of Computer Science in such a way that new resources and tools can be made available in a timely fashion;

- Network resources need to be protected from accidental and deliberate acts performed by those who have access to specialist ICT tools;
- Provision needs to be made to protect the performance and payment mechanism for network managers/service providers from acts that are beyond their control or where some risk has been accepted and responsibility acknowledged by the school leadership on behalf of the Computer Science teachers;
- A mechanism for regular review of the needs of Computer Science teachers and learners and the ability to change the contract or agreement if it's not meeting the needs of user or supplier;
- A strategy for managing the needs of Computer Science education needs to be defined at the highest level and needs to be risk based, using up to date technical and organisational controls; and
- The support provider and Computer Science teachers need regular professional development to cope with the rapidly changing technology.

1.1 Recommendations

School senior leadership teams should consider the following recommendations when considering introducing Computer Science to the curriculum:

- A strategy for Computer Science needs to be developed with a steering group representing all interested parties that regularly reviews the strategy and its implementation. This strategy should define the roles of those involved and their accountabilities;
- All technical solutions that facilitate the teaching and learning of Computer Science contain some risks and these need to be evaluated by someone with appropriate knowledge and the assessments should be discussed with all interested parties;
- School leaders need to decide which risks they are prepared to accept or transfer and what technical and organisational controls they are going to employee to mitigate the others;
- Technical solutions should be evaluated in light of technical risk, budget, support staff capability and teacher experience and preference;
- A change management policy should be created that meets the needs and concerns of teachers and network managers
- An acceptable use policy should be developed with students and should include references to the responsibilities of the students who have access to special ICT tools;
- Getting ICT technicians out into the classroom to provide support and to deploy, manage and store hardware would help develop understanding and trust;
- Teachers need continuing professional development to enable them to propose solutions that work for everyone and make efficient use of ICT resources;
- Support staff need continuing professional development to enable them to find solutions and implement them in a safe and cost effective way;
- Outsourcing agreements need to include flexibility and a mechanism for discussing and implementing technical solutions that are not pre-defined;
- Consideration should be given to the technical requirements of exam boards when choosing a syllabus for Computer Science as well as the teaching and learning needs;
- A well-documented approval process for installing new applications and a clear explanation of the costs involved can speed up implementation times and reduce conflict; and

- Clear, open and frequent dialog between those responsible for the running of the ICT infrastructure and those who use it has an important role to play in the successful implementation of Computer Science, more so than in other subjects.

2 Introduction

Computing at School (CAS) is a grass roots organisation, whose energy, creativity, and leadership comes from its members. It is a collaborative partner with the British Computer Society through the BCS Academy of Computing, and has formal support from other industry partners. Membership is open to everyone, and is very broad, including teachers, parents, governors, exam boards, industry, professional societies, and universities. CAS speaks for the discipline of computer science at school level, including FE, and not for any particular interest group.

Computer science has transformed the way we communicate, work and play in recent decades. However, it is not obvious to most people that it is a broad, deep, exciting, and fertile discipline. Its full potential can only be realised through great creativity and ingenuity in working with concepts, theories and challenges. It has also been a powerful source of new ways of thinking that have influenced many other fields, as diverse as biology, mathematics and philosophy. CAS aims to support and promote this vision of computer science in UK schools, by providing opportunities and resources to help all educators and learners to better understand, use and develop computer science in a variety of activities and fields.

CAS is supported financially by BCS The Chartered Institute for IT, Microsoft, Google, and the UK Committee of Heads and Professors of Computer Science.

This document is aimed at school decision makers who are considering introducing Computer Science into the curriculum and will also be a valuable reference for infrastructure providers. It describes the competing needs of the teachers and learners with the needs of the infrastructure service providers, whether they are school employed or an outsourced service provider. It explains the dilemmas and decisions school leaders need to make in striking the right balance between usability and security. It provides a set of generic solutions to the question; 'What ICT infrastructure options does a school have when considering teaching Computer Science?'

This whitepaper was inspired by Royal Society report of January 2012 entitled *'Shut down or restart? The way forward for computing in UK schools'*.[1]

In relation to school ICT infrastructure the Royal Society report said:

> **"School infrastructure service providers, working with others, should prepare a set of off-the-shelf strategies for balancing network security against the need to enable good teaching and learning in Computer Science and information Technology, and should encourage schools to discuss and adopt them with their service providers. Such a "Guide to Best Practice" should be used by schools and local authorities as part of any tendering process for outsourced service."**

It is hoped that this document will provide practical help to those wishing to embrace the teaching of Computer Science, those responsible for providing school ICT infrastructure and those entering into outsourced managed service contracts.

[1] http://royalsociety.org/education/policy/computing-in-schools/report/

2.1 Definitions

Computer Science is the study of the foundational principles and practices of computation and computational thinking, and their application in the design and development of computer systems. It is a subject discipline, on a par with Maths or Physics. A model curriculum for Computer Science has been developed by CAS.[2]

Infrastructure is used here to describe the school ICT network and its related component parts.

[2] http://www.computingatschool.org.uk/index.php?id=cacfs

3 Requirements and Challenges of Teachers and Learners

Teaching computer science involves the imparting of a set of skills and competencies but also the underpinning knowledge of how the concept of computation is played out in the real world. It is necessarily a practical subject that involves the use of computer resources which are both hardware and software that are already in use in school for a variety of purposes. There is a need to explore how computers communicate across networks and with locally attached peripheral devices. Learners need to experience practical problem solving to develop the associated learning.

3.1 Programming Languages

Teachers and learners need to be able to use several computer programming languages that demonstrate the different language types available. For example; imperative, declarative and functional. What languages are used is a matter for the teacher and their background as they are going to need to teach in a language which fits their experience and competence. Much of the programming software and associated material that is available for Computer Science teaching is either completely license free, is open source or has a licensing scheme for education that is cost free like the Microsoft Dreamspark programme that is free to CAS members[3], consequently there is no per user or station cost for software licences but only the cost of installation and maintenance. There is also a core requirement by the exam boards for some course work that is carried out within one of a set of prescribed languages (there is a list of accepted languages published by the boards an example of which is given in the Appendix). Which language is used will need to be decided by the teacher responsible for teaching the course.

Alongside the programming language there will be some form of development environment. Again, which one depends on the teacher, which language they have chosen to teach and there may be several. For example, in a Java based course a teacher might want students to be able to compile and run code from the command line in order to get them to understand the processes that lead from a source file to a runtime executable. This might be followed by using Greenfoot[4] and/or Bluej[5] to develop programs for most of the course. Some teachers might want to use Netbeans[6]or Eclipse[7] as these are widely used platforms in industry. Once they have created their executable code, the student needs to be able to run it, debug it and run it again.

3.2 Workstation and Network Environment

When students are developing software they will invariably create programs that stop responding and halt the execution of the machine they are working with and so they will need to be able to kill whatever process has caused the problem ideally without having to reboot the workstation they are using.

When carrying out coursework, students will need to be able to manage their files in such a way as to obey whatever rules the exam board might put in place. The way workstations and the network is configured needs to accommodate this as it is unlikely that the teacher will be able to manage this themselves (e.g. via a box full of USB memory sticks.). The storage and movement of files from

[3] http://www.dreamspark.com
[4] http://www.greenfoot.org
[5] http://www.bluej.org
[6] https://netbeans.org
[7] http://www.eclipse.org

development environments to backed-up work areas is a requirement across lots of subjects and so should not be a computer science issue.

When demonstrating aspects of Computer Science, the teacher needs to be able to demonstrate aspects of workstation management such as installing and removing software and accessing the state of the machine in the form of memory contents and settings. They need to be able to access a list of running programmes and review the resources they are using. They may also need to be able to run network packet capture and analysis and run network troubleshooting and information gathering tools. At A-level or within other Level 3 courses, students may need to access profiling software to analyse how their program is working. In particular, within vocational courses this may be part of IDEs such as Netbeans, XCode[8] or Microsoft Visual Studio[9].

3.3 Access to files

When working from day to day students need to be able to manage the versions of the program they are working on. They will probably have at least one major project that they are working on both at school and at home. They need to be able to access their work for Computer Science from both within and outside the school or college without having to carry versions around on USB memory sticks. A version control system is also an important aspect of helping them progress as well as being an important aspect of their learning. Some vocational courses use version control systems such as Git[10] as an important resource in teaching and learning as well as an excellent way of enabling students to manage their projects.

3.4 Hardware

There will be a section of most courses that involves hardware and a teacher might require the ability to manage devices such as robots, for example Lego Mindstorms[11], networking devices, input devices such as the Microsoft Kinect for Windows[12] and single board devices such as a Raspberry Pi[13] or an Arduino[14] boards.

3.5 Operating Systems

The teacher will want to be able to demonstrate different operating systems such as Linux, BSD Unix, Microsoft Windows and Apple OSX as well as mobile operating systems like Android, iOS and Windows Phone. The way this is done needs to make the authentication of users and connections to home directories work correctly so that files and information can be easily transferred from the test system to the live network environment.

3.6 Infrastructure Challenges for Teachers

A Computer Science teacher in a school will be faced with some challenges when negotiating with their ICT support team over the way the school ICT infrastructure is setup and managed. With an outsourced ICT service they may face some specific challenges with the way the contract under which the managed service provision is negotiated. Any support service will have to cope with the

[8] https://developer.apple.com/xcode
[9] http://www.microsoft.com/visualstudio/eng/products/visual-studio-overview
[10] http://git-scm.com
[11] http://mindstorms.lego.com/en-gb/default.aspx
[12] http://www.microsoft.com/en-us/kinectforwindows
[13] http://www.raspberrypi.org
[14] http://www.arduino.cc

changes required to teach Computer Science. If it is provided by a 3rd party it will almost certainly have a formal 'change request' provision and a mechanism whereby changes to computer setups can be made, albeit sometimes at a cost. The experience of many schools under the Building Schools for the Future programme for example was that the terms of the contract were not clear to the schools involved and certainly not to the teachers who were actually receiving the service. The negotiations of the IT services terms were a small part of the overall BSF project and the eventual provider was often determined by the scoring under the main contract without the needs of the Computer Science teachers featuring very prominently if at all.

A challenge may present itself when the contract is 'a full transfer of risk for ICT from the school' if the teachers have subject specific requirements from the ICT infrastructure. The risk management strategy lies with the supplier rather than the receiver of the service and such subject specific requirements may be perceived as high risk to the supplier.

Amongst the many potential sources of conflict is where a teacher, who wants to implement a new teaching strategy, ends up in a lengthy process of risk management when all they want to do is focus on teaching and learning. The teachers' perception is that the process is generated by the IT manager or service provider in the school, at best as a way of opposing change and at worst to prevent the time and effort being expended in changing the stable system that they have implemented.

Other sources of conflict include:

- The technician on-site might have views about the way in which the teacher is using the network and hardware that are not shared in a constructive way or there is no forum for expressing such concerns;
- The use that teachers and students need from this equipment may have the potential to disrupt others' use of it; and
- The costs quoted for resolving problems are given in terms of per student or per computer costs for the whole school when most of the pupils will never use the facilities anyway.

As far as the teacher is concerned the infrastructure provider is primarily a service provider and they expect them to provide networking and processor power on-tap when they (the teacher or students) want to use it, for whatever reason they may need to. Teachers assume the service should be provided in much the same way that their utility provider supplies energy, without unduly interfering with how customers use it. These expectations may not reflect the different types of contracts that are in place.

Where solutions are offered, there is sometimes a 'gotcha' that makes the proposed use so inconvenient as to render the teaching and learning all but impossible. For example, groups of non-networked machines being the only ones offered for teaching Computer Science or special login IDs using different passwords that prevent the user tying together work from one account to another. Perhaps as an alternative the insisting on using 'lite' or otherwise limited versions of particular languages that are 'approved' by the service provider. One of the biggest challenges is a complex approval process that can take several years to complete by which time the group that originally wanted the facilities for their teaching and learning have moved on to an alternative, less desirable but easier to implement solution. It is certainly the case that teachers, having looked at the

restrictions placed on using IT in a particular school, have decided to withdraw from their application to teach there.

A Computer Science course is a course about how a computer works rather than what applications we may run on it from time to time. To write down what teachers and students need is rather difficult and it might be easier to define what they don't need? A great deal of use is rather specialised and technical and may be confined to the teacher using their school laptop leaving the students to work on their own devices.

Good teaching and learning relies to a great extent on the enthusiasm of teacher and that enthusiasm often stems from the way they want to teach. Their methods may be idiosyncratic but they represent the needs of the school that should have been in the contract output specification in the first place.

4 Requirements and Challenges of Infrastructure Service Providers

Schools' ICT infrastructure is procured, implemented, configured and maintained in a wide range of settings by a large variety of in-house and 3rd party providers in a seemingly infinite number of ways. Some of those responsible for the ICT infrastructure are direct school employees, some are local businesses or volunteers and some are large managed service providers. Each faces similar challenges when it comes to balancing the needs of the educators, students, administrators and managers with the requirement to maintain the availability, integrity and confidentially of the school network. The way each network manager, infrastructure or service provider operates may differ as they are driven by different types of contracts that measure their performance in different ways.

The use of managed service providers to provide and manage school ICT networks over the last decade increased for a variety of reasons including the existence of the Becta Infrastructure Services procurement framework (now replaced by the DfE ICT Services Framework)[15], the awarding of various Private Finance Initiative projects and the former government's Building Schools for the Future programme.

When a managed service provider is engaged, a contract is entered into between the provider and the procuring body which defines the level of risk transfer. These contracts have a payment and performance mechanism that ensures the provider is focused on delivering a specified level of service by financially penalising them when they underperform. There are a variety of key performance indicators for managed service providers and the main one is often ICT infrastructure availability. This reflects the increased reliance that schools place on their ICT to run their school as a business as well as educate their students. This drive to maximise availability has given rise to conflict in some cases where the needs of educators wanting to teach Computer Science are not clearly defined in the output specification or contract requirements.

The challenges are also keenly felt by those who are employed directly by schools to provide and maintain the ICT infrastructure as they are there to provide the same professional standards and levels of service, often with fewer resources at their disposal, while supporting and facilitating teaching and learning. They may feel the pressure even more keenly as they are governed by terms and conditions of employment that also don't reflect the conflicting requirements of network users and Computer Science teachers yet they are expected to respond to the direct and often ad hoc requests of colleagues.

4.1 What Are the Risks to the Service Provider?

Being an effective ICT infrastructure provider, either as a direct employee of the school or an external organisation, is a question of balancing risk. This is the risk that allowing Computer Science students to perform actions that other users don't need to perform may cause problems for all network users. This risk problem is no different in reality to that faced by the managers of IT in corporate settings where there are software developers or network engineers using the same infrastructure as their non-technical business colleagues. The difference is that the corporate environment can spend considerable sums of money creating the right environment for all ensuring critical business functions are not disrupted. With revenues and profits to protect a business can

[15] http://www.education.gov.uk/schools/adminandfinance/procurement/b0069801/buying/ict/ict-services-framework

justify the expenditure. In a not-for-profit environment there will be other legislative pressures and corresponding funds to ensure a similar robust and appropriate ICT resource is provided.

School staff are familiar with the concept of risk assessment, for example when taking students out of school on a trip or carrying out some practical activity in lesson time. When managing the ICT infrastructure the responsible person also needs to carry out risk assessments on a daily basis. The network infrastructure in schools today is very complex and on a par with a medium to large sized business but may employ technologies more commonly found in larger enterprises. There will be solutions in place that are unique to the education arena due to the unique demands of the users, for example the common practice of each student using several different workstations during the course of a single day and needing to access the same resources wherever they are. All of the component parts of the infrastructure from the broadband router to the software that comes with the printer have inherent vulnerabilities that need to be understood and managed. Without adequate controls in place, as identified by a risk assessment, the infrastructure's weaknesses may be exploited and problems may arise.

Most ICT service providers to businesses are mainly concerned with computer exploits originating from outside of their organisation. Schools are unusual in that there are as many, if not more, attacks on the infrastructure, be they deliberate or accidental, from within. These attacks or exploits can take many forms including:

- Viruses or malicious software designed to steal or change data or make systems unstable;
- Hardware and software systems designed to steal passwords or impersonate one user while connected as another such as keyloggers;
- Software tools and configurations designed to bypass the normal access and filtering controls such as web proxy servers; and
- Software applications that can disrupt the availability of the network for other users if used carelessly or inappropriately such as a DHCP server.

These may lead to information security or safeguarding incidents. Personal or financial information could be at risk and students may become exposed to e-safety risks that the schools systems are designed to guard against. Educational establishments are also susceptible to the users wanting to waste time and play computer based games which are accessed via web sites or locally installed executable code. A school's duty of care also needs to take into account young people's ability to take excessive risks and of finding new and novel ways to harm themselves accidently or deliberately. While an appropriately configured and maintained infrastructure, along with suitable training and acceptable use policies, will minimise the risk of such incidents occurring there is a danger of the network being so tightly controlled that it impedes the needs of teachers and learners.

In the majority of cases these exploits are carried out using executable code introduced deliberately or accidently from outside of the network. Sometimes the code comes into school on removable drives, sometimes in email attachments and sometimes from web sites. It is also possible that a student may create malicious code themselves. It is therefore necessary for the service provider or network manager to limit the ability of users to run executable code to only those which they need to run, as defined by the acceptable use policy, and are deemed safe to do so such as curriculum and administration applications. This can be at odds with the teaching of Computer Science as one of the

key objectives is to teach students how to create and run executable code that is neither irresponsible nor malicious.

4.2 Reducing Risk

At one extreme the majority of the risk to the infrastructure can be removed by 'locking down' the system so the users have limited access to a restricted set of functions that allows them to do their work while removing any flexibility they have in the way they accomplish their tasks and limiting the amount of change that can be requested. Best practice, as recommended in ITIL[16] and ISO/IEC 20000[17], deems that any changes that are considered necessary be rigorously tested to ensure no new vulnerabilities are introduced. This approach is desirable from the provider's point of view as it means their infrastructure remains stable, predictable and highly available and the support burden is minimised. For teachers of any subject that wants access to new resources and applications this can be very frustrating but especially so for those teaching Computer Science because it can prevent access to the very functions they are trying to teach.

At the other end of the spectrum the maximum amount of flexibility and freedom can be provided by giving all users full access to all functions with no limit on the changes they can make. This is often the approach taken with home computers where all family members have 'administrator level' access. This makes the computer easy to use without restrictions 'getting in the way' but it is a risky strategy especially for non-technical users. This can add to the frustration of teachers as they are used to being able to do tasks at home that they may not be able to do at school.

There is a middle ground as with any risk management problem. School leaders need to decide how much risk they are prepared to accept and what technical and organisational controls they are going to employee to manage them in conjunction with their support providers and within whatever contract limitations exist.

[16] http://www.itil-officialsite.com
[17] http://www.isoiec20000certification.com

5 School Management Issues and Potential Solutions

There does not appear to be a consistent approach to the management of ICT systems or the associated support staff within UK schools despite the efforts of Becta and others to introduce the *Framework for ICT Technical Support* (FITS)[18] as a model for best practice based on the industry standard *Information Technology Infrastructure Library* (ITIL). The role of the ICT support staff varies as much as the technology they support. On the other hand, there is a pretty standard model for the management of the teaching staff in a hierarchy of Senior Management, Heads of Faculty, Heads of Department and Teachers. Most of these groups do some teaching.

The traditional school network manager will fit alongside this hierarchy as a provider of a service in much the same way as a Bursar, Estate Manager or Catering Officer and, as such, will (generally) report to a member of the Senior Management Team and ultimately, the school Governors.

In the event that the school has bought into an ICT outsourcing arrangement, which may or may not include outsourcing facilities management, the management of the Network Manager and the ICT technicians usually lies with the outsource company via the TUPE process[19]. The interaction of teaching and non-teaching staff with that third party company may lie with the network manager and his colleagues or partly through them and partly through some form of first line support desk. This arrangement often results in the same people being employed in the same roles in the school but now the ICT technical support staff report to a different employer. The relationship with the teachers may change as a result and informal agreements between teaching and non-teaching staff will be replaced by the service provider's way or working which has been developed in response to the SLA that the outsourcing contract has brought about.

At the time of the new contract being introduced a new network management framework may also have been introduced along with new technology. Some outsourcing contracts will bring with them a more formal approach which may be more in-line with FITS or ITIL than was previously the case in the school and all the staff will need to adjust to this as their roles and the way they interact with each other changes.

5.1 Key Roles

The main role that oversees the day to day teaching of ICT is usually that of the ICT Coordinator. This is a post that used to exist in almost all schools and is still common in primary schools. Their role, simply put, is to encourage and advise teachers who are using ICT in their lessons. There are now many more teaching assistants in this evangelising role who have the time to be in various classes assisting with the use of technology.

This supporting and encouraging role may be combined with the head of the IT department, who may be a member of the senior management team and they will be a key source of advice to the school in making decisions relating to ICT initiatives like the introduction of the teaching of Computer Science.

The main non-teaching role is that of the Network Manager. This role has gradually become more professionalised over the past 20 years or so. The post has grown as networks and the complexity of

[18] http://www.thefitsfoundation.org
[19] http://www.lge.gov.uk/lge/core/page.do?pageId=119763

the networks they manage has grown. Their qualifications and expertise vary enormously and their role is key in the success of using ICT in teaching and learning. They may report to the senior management team, a committee, the ICT Coordinator or the outsource service provider operations manager/team leader. They may themselves have a number of direct reports who either assist in running the network or have specialist functions like managing the MIS system, email system or school web sites.

5.2 The ICT Infrastructure

Unless a school has had a major refurbishment or new build, the ICT infrastructure is likely to have evolved over a decade or so. Schools have undergone huge changes in direction in that time and much of that change has not gone hand-in-hand with the redesign and re-equipping that might have been warranted in ideal circumstances.

The school should have a programme of technology refresh, renewals or some other program of updating equipment once it is no longer secure, economically viable to support or no longer meets the needs of the users. This however is not guaranteed.

Modern school ICT systems are complex and often the equivalent to a medium sized enterprise. It is beyond the scope of this document to detail school ICT systems but when considering the challenges associated with teaching Computer Science it is useful to consider two main categories of computer resources; teacher devices and student devices. Teachers usually have their own device that travels around with them or is exclusively for teacher use and students usually travel to a place where they use a device. This is however changing as more and more new devices are mobile and over time 1:1 personal devices will become a reality and eventually we may get to a point where users just reach for the nearest browser.

Teachers are using their ICT capacity to experiment, inform and support their teaching and there isn't any easy way of predicting how they will want to use it. If they find that they cannot use the equipment in the way they want then they will either bypass the official systems in some way or not bother using them.

If a service provider tries to predefine every use-case of the equipment in order to guarantee stability they may end up with frustrated teachers that will just do things differently. If the system is sufficiently robust to give them freedom to innovate, the service provider might find that their service is used more effectively and with more enthusiasm.

Where student devices are shared, it is important that everyone who sits down to use them should find a consistent environment. This, coupled with the fact that the devices are not customised to a particular person's work needs, makes the locking-down of general purpose workstations almost inevitable.

5.3 Sources of Conflict and Possible Solutions

The differing needs of teachers and learners and the demands of the rest of the school population together with the outsource service level agreement or expectation on the Network Manager inevitably leads to some conflicts that need to be addressed. Here are some examples:

- *A teacher is told that their project cannot be implemented straight away* – teachers of many subjects including Computer Science need a clear change control process in place so that they can plan and implement teaching and learning projects in reasonable timescale. Ideally within one term but certainly by the next academic year.
- *A teacher is told that their project cannot be implemented for some reason* – where the service provider finds they are unable to provide the service, there needs to be a clear reason for the problem and some real engagement with what the teacher wants to do. In other words, teachers should be able to talk to the service provider about what they want to do and why. Sometimes teachers gets vague 'security related' excuses rather than solutions to their problems. If there are security concerns they need to be explored in the risk management context detailed below.
- *A teacher is told that their project is inappropriate* – what constitutes good teaching and learning is a matter for the educationalists and the technical staff should point out the risks whilst being neutral on what they think the educational value is.
- *A teacher is told that their project is too expensive to implement* – whilst this may sometimes be the case, the response needs to be properly quantified and be part of the change management process. The service provider has to think about and report on how these costs are derived. That is not to say that they can't put a price on it. Teachers need to understand that change costs money.
- *A teacher is told that their project can only be implemented after they go through a complex risk management process* – whilst the IT management process should include risk analysis, it is neither the duty of a teacher to carry out the risk analysis nor is it within their capability. It is perhaps reasonable to get the teacher to make a case in a single page document. Beyond that, it just looks like the Network Manager is being deliberately obstructive.

5.4 A Strategy for Computer Science

Creating an environment in which Computer Science can be taught requires strategic leadership. This needs to be endorsed if not led by the senior leadership team as it will need to bring together all the groups involved that may not all sit under the same management reporting lines. As with any subject that requires access to scarce or competing resources a business case for Computer Science needs to be established. A Computer Science steering group is one approach. It can review all the competing issues and opinions and this may need to include a representative of the managed service provider if appropriate. This group can decide how to implement the objectives of the business case that has been approved and may even create the business case in the first place. The steering group can provide the means by which objections can be aired and conflicts resolved and it can determine priorities. The steering group needs to represent the interests of the technical support team as well as the academic team to be successful.

A strategy for Computer Science should include regular reviews and convene the steering group several times a year because of the rapid advances in computer technology. This group can review the following:

- Current and future hardware and software resource requirements;
- Special network configurations required for the teaching of Computer Science;
- What is acceptable use of ICT resources by pupils;

- The risks associated with the required set-up;
- Inputs to the change management process; and
- Issues arising.

5.5 Acceptable Use

There is likely to be a policy body of some kind within the school that determines such things as Acceptable Use Policies (AUPs), e-safety policies and spending on long term IT projects and how they can be funded. This committee may have a senior member of staff on it or may not.

Acceptable use is a whole-school issue. The aim is to create a culture where sensible use is promoted by all. At its heart is the negotiation of an acceptable use policy understood by all whose purpose is to come to a shared understanding of what is, and is not acceptable. This should be built, through discussion and debate, and couched in a language that is clear to all. The policy should be simple, concise and framed with reference to the schools core values.

Some children, in particular the technically savvy, may think normal mores are suspended to some degree when using computers. The budding hacker may gain pleasure in finding security flaws, but would baulk at the suggestion that it is akin to prowling the grounds looking for an open window. This is the real challenge – trying to instil the same moral understanding to digital behaviour as exists in the real world.

Potential for misuse will always exists, but malicious incidents should be rare. By using an appropriate logging and auditing system the responsibility for IT issues, malicious or accidental can usually be pinned down to whoever is accountable. This accountability is an important educational outcome as well as being useful to the service provider.

A well written AUP can foster an environment in the school where malicious or inappropriate use of IT is rare. Arguably, it is as important to have a well-supported and developed AUP system as it is to have well developed infrastructure support.

Such an approach can only be possible where the technical support team has a clear understanding of the student's requirements and the teachers have a clear understanding of the security concerns raised by technical support. No doubt requirements will change over time and new solutions will need to be developed in response. If the AUP is developed and used sensibly, it will be supported by everyone including students and Computer Science students are particularly well placed to help 'police' the network, reporting any concerns.

5.6 A Risk Based Approach

The details of a risk management process are beyond the scope of this document, however if there is a well-designed risk based framework for evaluating security the users will enjoy a greater degree of freedom and flexibility than might otherwise be the case.

Each proposed technical solution or change to the infrastructure needs to be assessed by an appropriately skilled and experienced person. The outcomes of the assessment can be shared with the management team, teacher requesting the change and the technical support team. A risk-averse leadership team may only accept a situation where the probability of something going wrong is low and the impact is also low. Where the right culture exists a more relaxed approach may be possible.

In practice a combination of technical and organisational policy controls will be employed to minimise risk as far as is reasonably possible for high and medium impact situations. An example might be to only allow students to run executable files inside a virtual machine that can't communicate with the rest of the network because the probability that they can compromise the rest of the network will be significantly reduced by doing this. However, stopping the running of files does not have to mean that students cannot then store their work inside their home directories.

Computer networks can be configured in many ways and by regularly attending recognised training courses provided by vendors like RM[20], the support team can be aware of the risks, standard approaches and common pitfalls. In-house support staff can also take advantage of courses and certifications provided by Microsoft if the school subscribes to the IT Academy programme[21] which provides a wide range of resources and materials that could benefit them as well as teachers and students.

5.7 Change Control

Change control is an essential process in any network management environment. It is a formal process developed to ensure that changes to the infrastructure are introduced in a controlled manner thereby reducing the possibility of introducing inappropriate changes. The aim of a change control process is to minimise disruption to services, ensure that new services are implemented in a cost effective manner and that the infrastructure remains robust and secure.

Change control is necessary regardless of who is managing the network. In an outsourced environment it usually works at two levels. At the contract level formal change notices can be agreed which override the original contract wording and will be agreed by the service provider and customer and will be written by lawyers. These types of change are usually rare as everyone wants to avoid the hassle and expense.

The other type of change happens at the school or LA level and the process for this will be defined in the contract. This usually follows ITIL best practice where a change is requested, evaluated and then raised at a change advisory board. If the change is considered acceptable by all sides it will get approved and implemented. Some of these changes will be chargeable because of the amount of effort involved or because additional hardware or software licences need to be acquired. Some change will be free to the customer. There will also be a set of standard changes that can be requested that are usually free and pre-approved and these will be defined somewhere. Overall, the process must take place in an acceptable timeframe.

An example of contract level change might be the dropping of one contract performance measure and replacing it with another which benefits both supplier and customer whilst maintaining the overall level of risk transfer. An example of a non-standard change that needs to be approved might be a change to a firewall rule to allow access to a new service. An example of a standard change might be the adding of a new printer.

[20] http://www.rm.com/shops/solutionsandservices/Catalogue.aspx?nguid=8d48de50-86ef-4d57-ab5e-c783be42f86a&rfr=homemnutxt
[21] http://www.microsoft.com/en-us/itacademy/default.aspx

A school wanting a new programming environment installed on the network could fall into the non-standard change if it's complex and needs technically validating or it could fall into the standard change category if it's a simple application to install.

Whether change management is an issue for schools depends on how long it takes to get changes processed and whether they are charged for them and this depends on the contract and how it's managed. Changes are more likely to be agreed to if there is a precedent and the request is made in plenty of time. Good change control depends on good communication from both sides and is possible where both sides work in partnership.

Both sides of the contract have an interest in good change control. Teaching and learning will be well supported if teachers can implement innovation in a controlled way. Similarly, service providers will have happier customers and more chance that the contract will be renewed at the end of its term.

6 Possible Technical Solutions

This section will look at the available technical solutions that support the teaching of Computer Science in schools. The table below details the various types of solution based on the level of expertise required to implement and maintain them. It also attempts to give an indication of the level of complexity associated with using the various types of solutions. This is an important factor and the type of technology employed will come down to how the following questions are answered.

- What programming languages and additional hardware does the teacher want to use?
- How much interaction with the school network do the learners need, for example to access the internet and save completed work and work in progress?
- What technologies can the school support staff manage?
- What existing hardware does the school have that could be used to run computer science lessons with?
- How much budget does the school have to spend on Computer Science?
- How much risk can the school manage either alone or with the help of a service provider?

Technology alone is never the answer to information security risk management and neither is it the sole answer to providing a secure programming environment in school. Choosing a technical solution is part of the task. Defining and implementing policy that supports the solution is the necessary other part of the equation.

Which technical solution a schools chooses will partly depend on their appetite for risk and this in turn depends on the culture of the school. In some cases a more open and flexible technical solution will work accompanied by an appropriate level of trust in the network users supported by a good working set of policies. In some cases a risk free and tightly controlled solution will suite where local expertise is not so readily available or in some cases where the solution is outsourced and the contract requires it.

7 Table of Possible Technical Solutions

	Type of Technical Solution	Advantages	Disadvantages	Complexity to implement and maintain	Complexity to use	Examples
1	Development using scripting tools built into the operating system.	Ease of use. No setup costs. Multiple languages can be taught. Cross-platform.	Some functions may be restricted to protect the integrity of the computer or network. The OS might have a very limited set of tools available.	Very Low	Very Low	Javascript development using a text editor and a web browser.
2	Web based development environments that don't need anything extra installed or configured on the school network or end user devices.	Ease of use. No setup costs. Multiple languages can be taught. Cross-platform.	User's work is stored in the cloud so care needs to be taken to ensure work is backed up. Limitations on what can be taught/developed. May not conform to exam board requirements for course work.	Very Low	Very Low	http://www.codeacademy.com

	Type of Technical Solution	Advantages	Disadvantages	Complexity to implement and maintain	Complexity to use	Examples
3	Web based development environments that need specific browser plugins.	Ease of use. No setup costs. Multiple languages can be taught. Cross-platform.	User's work is stored in the cloud so care needs to be taken to ensure work is backed up. Limitations on what can be taught/developed. Plugins need to be installed and maintained on workstations.	Low	Low	http://www.yousrc.com
4	Self-contained development environments that are installed in the same way as any other application and don't require special conditions to run code written.	Easy to setup. Provides most of the features teachers and learners need for traditional development.	Limited to a platform specific set of programming languages.	Low	Low	• Greenfoot (http://www.greenfoot.org) • BlueJ (http://www.bluej.org) • Alice (http://www.alice.org) • Scratch (http://scratch.mit.edu) • Kodu (http://fuse.microsoft.com/projects/kodu) • Microsoft Small Basic (http://smallbasic.com/)

	Type of Technical Solution	Advantages	Disadvantages	Complexity to implement and maintain	Complexity to use	Examples
5	Development environments that can be installed as above but do need special configurations to work e.g. special permissions to be set for the users.	Provides most of the features teachers and learners need for traditional development.	Limited to a platform specific set of programming languages.	Medium	Low	Microsoft Visual Studio Express (http://www.microsoft.com/visualstudio/eng/products/visual-studio-express-products)
6	Development environments that can be installed with or without special configurations but then use an emulator which may or may not need to be installed separately to run the finished code.	Provides most of the features teachers and learners need for traditional development. Uses a hardware device or emulator increasing interest	Limited to a platform specific set of programming languages. Uses a hardware device or emulator increasing complexity	Medium	Medium	MIT App Inventor (http://appinventor.mit.edu)

	Type of Technical Solution	Advantages	Disadvantages	Complexity to implement and maintain	Complexity to use	Examples
7	Development environments where the finished code is run on dedicated hardware separate from the normal school network.	Provides most of the features teachers and learners need for traditional development with the added interest of the associated hardware	Limited to a platform specific set of programming languages. Needs associated hardware.	Medium	Medium	• Lego Mindstorms (http://mindstorms.lego.com/en-gb/default.aspx) • Raspberry Pi (http://www.raspberrypi.org/)
8	Application virtualisation solutions that packages and delivers a development environment in a sandbox. May also provide the ability to run the application from a removable drive.	Provides most of the features teachers and learners need for traditional development. No special hardware requirements on student computers.	May require some additional software and infrastructure to setup. Transferring work outside of the virtual environment adds complexity.	High	Medium	• Microsoft App-V (http://www.microsoft.com/en-gb/windows/enterprise/products-and-technologies/virtualization/app-v.aspx) • VMWare ThinApp (http://www.vmware.com/products/thinapp/) • Numecent Application Jukebox (http://www.numecent.com/products/application-jukebox.html) • Cameyo (http://www.cameyo.com/)

	Type of Technical Solution	Advantages	Disadvantages	Complexity to implement and maintain	Complexity to use	Examples
9	Virtual machines setup on classroom PCs that allow the students access to a full development environment with some restrictions in place to prevent undesirable interaction between the developed code and the host environment.	Each student has full access to a dedicated virtual computer with all the development tools installed for that platform. Provides a balance between security and usability.	May require some additional operating system licences and higher specification workstations. Transferring work outside of the virtual environment adds complexity.	High	Medium	• VMWare Player (http://www.vmware.com/products/player/) • Oracle Virtual Box (https://www.virtualbox.org/) • Microsoft Virtual PC (http://www.microsoft.com/en-gb/download/details.aspx?id=3702) • Parallels Desktop for Apple (http://www.parallels.com/products/desktop/)

	Type of Technical Solution	Advantages	Disadvantages	Complexity to implement and maintain	Complexity to use	Examples
10	Dual boot computers with a normal operating environment in one partition and a development environment in the other with limited interaction between the development environment and the rest of the infrastructure.	Each student has full access to a dedicated computer with all the development tools installed for that platform.	May require some additional operating system licences. Transferring work outside of the development environment adds complexity although the same user credentials can be used in both environments.	High	Medium	Windows, Apple OSX or Linux operating systems
11	Access to an on-premises web server so that students can develop code to run in their own web site on the shared web server.	Each student has full access to a dedicated web server with all the development tools installed for that platform.	Limited to web based programming on one platform. Needs appropriately configured server software and possibly extra hardware.	High	Low	• Windows server with SQL and .Net • Linux/Apache /MySQL/PHP

	Type of Technical Solution	Advantages	Disadvantages	Complexity to implement and maintain	Complexity to use	Examples
12	Access to a cloud based web server so that students can develop code to run in their own web site on the shared web server.	Each student has full access to a dedicated virtual web server with all the development tools installed for that platform. Management of the environment is less of a burden.	Limited to web based programming on one platform. Need to pay a service provider. Possible issues with course work authentication.	Medium	Low	Most web hosting providers that offer advanced hosting packages
13	Standalone or networked 'unmanaged' computers used for software development that can be easily returned to their predetermined clean state after use.	Each student has full access to a dedicated computer with all the development tools installed for that platform.	Students need to remember to copy their work elsewhere at the end of each session. Dedicated computers required. Students have to cope with multiple login credentials and complex backup processes.	Medium	Medium	• Windows, Apple OSX or Linux computers • Raspberry Pi

	Type of Technical Solution	Advantages	Disadvantages	Complexity to implement and maintain	Complexity to use	Examples
14	Low cost mobile computers in a 1:1 computer to student ratio provided by the school or as part of a BYOD programme	Each student has full access to a dedicated computer with all the development tools installed for that platform. The student can work on projects at any time. Cost may be borne by student.	Devices may not be powerful enough for some tasks or limited to which development environments they support. Potential lack of consistency of experience. May require expensive wifi infrastructure.	Medium	Low	• Windows, Apple OSX or Linux computers • Raspberry Pi
15	Virtual desktops configured for software development that are hosted in a virtual desktop infrastructure that is hosted in-house.	Each student has full access to a dedicated virtual computer with all the development tools installed for that platform.	Needs appropriately configured server software and extra hardware.	High	Low	• Citrix XenDesktop (http://www.citrix.com/products/xendesktop/overview.html) • Microsoft Windows Server 2012 (http://www.microsoft.com/en-us/server-cloud/windows-server/windows-server-2012-r2.aspx) • Oracle Virtual Desktop Infrastructure (http://www.oracle.com/us/technologies/virtualization/virtual-desktop-infrastructure/overview/index.html) • Red Hat Enterprise Virtualization (http://www.redhat.com/products/cloud-computing/virtualization/) • VMware View (http://www.vmware.com/products/horizon-view)

	Type of Technical Solution	Advantages	Disadvantages	Complexity to implement and maintain	Complexity to use	Examples
16	Virtual desktops configured for software development that are hosted in a virtual desktop infrastructure that is hosted in the cloud.	Each student has full access to a dedicated virtual computer with all the development tools installed for that platform. Management of the environment is less of a burden.	Need to pay a service provider.	High	Low	• Citrix XenDesktop • Microsoft Windows Server 2012 • Oracle Virtual Desktop Infrastructure • Red Hat Enterprise Virtualization • VMware View • Microsoft Azure (http://www.windowsazure.com/en-us/) • Amazon AC2 (http://aws.amazon.com/ec2/)

7.1 Preventing the Running of Executable Files

The ability for students to be able to run executable code they have written is key to the teaching of Computer Science and will be an important consideration for any technical solution. This can be provided in many several ways.

Some school networks employ a Microsoft networking technology called 'Software Restriction Policies' first introduced with Windows XP and Windows Server 2003. This creates a set of editable policies that determine what executable files users can run and where they can run them from. There will usually be a set of default software restriction policies that allow a user to run applications that are installed on their workstations and those that run directly from the server. The policies can be edited by the network manager to add additional files and paths. When a new software package is added to the network the appropriate software restrictions are modified, if necessary to allow the new application to run.

The use of these policies, in addition to a set of permissions on files and folders and not having users logon as admin level users, goes a long way to preventing viruses spreading throughout the network as they prevent users from inadvertently downloading and running malicious code from drive-by download infected web sites or from infected USB memory sticks which together make up the majority of the virus ingress points. There will of course be the occasional enterprising student who makes their own malicious code or downloads something from the internet at home and brings it in to school and tries to run it on the network. This will be blocked by correctly configured software restriction policies.

From the network manager or service provider's perspective 'hiding' certain parts of the workstation and server file system and not allowing students to run executable files they create themselves helps to preserve the availability and integrity of the network and reduces the chances of students going off task. From the teachers and student perspective it may seem unnecessarily restrictive unless managed well.

7.2 Access to the Command Line Interface

Similarly access to the command line is usually considered a requirement of any technical solution designed to support the teaching of Computer Science. As with running executable files the attempt to hide the feature from regular network users is only part of the solution and not the whole answer.

Good security policies should be built on the assumption that all measures to secure the network are known to any 'adversary'. This is the model used by NIST for approved cryptography solutions[22]. The encryption algorithms are publicly documented and the only necessary secret being the key. A similar approach needs to be made to the command line interface and whether it is acceptable to give students access to it or not. The assumption in this case is that they will find a way to get there sooner later so rather than try and implement 'security by obscurity' and hide the command line interface, we should control what they can do when they do have access to it.

In the case of up to date operating system installations command line access from a securely configured workstation shouldn't cause any problems, in the case of Microsoft Windows, the file system and registry will be locked down by permissions and access to network commands (net.exe,

[22] http://csrc.nist.gov/groups/ST

etc.) can be denied to users via permissions and software restriction policies. It is likely that a knowledgeable user will be able to access the command line and the infrastructure provider should be working on the assumption that this is the case.

8 Appendix 1 – AS/A Level Computing Requirements

8.1 AQA AS/A Level Computing Requirements

The following information relates specifically to the AQA AS/A Level Computing[23] examination and will be similar for other exam boards. (See Appendix 4 for details of exam board offering Computer Science or Computing GCSE and A-Level)

AQA AS level candidates are required to sit a practical exam which at the time of writing is offered in two versions of Visual Basic (VB6 and VB.net 2010), two versions of Python (2.6 and 3.1), a version of Java (the current one) and a FreePascal/Delphi version (centres are allowed to make minor alterations to the supplied test program code in order for this code to work with the version of Pascal that is used in the centre). Centres choose which programming language(s)/version(s) they wish their students to use in the practical exam from the available versions. FreePascal/Delphi generates executables when the source code is compiled.

It is also desirable but not essential that AS Level students benefit from having hands-on access to a local web-server (for example Apache or Microsoft Internet Information Server) that they set up/configure on their networked workstation, an FTP client for uploading web pages to the local web server, an FTP server that can be set up/configured and run by the student on their networked workstation, a local database server (for example MySQL, Interbase) that the student can set up/configure on their networked workstation, access to a telnet client/server system (or ssh client/server). In some centres the web server, database server are already installed on each networked workstation ready for the student to configure.

Students also need access to a command line, in order to be able to do practical work in networking commands such as using commands such as ping, dig, netstat, nbstat etc.

In the second year of the course (A2) students study for the A Level. They are assessed by a project and by a written paper exam. The project is a substantial piece of work involving programming a solution to a problem that may be of the student's choosing. Students may generate executable code (exe's) as a natural outcome of this project work because they use a programming language that compiles to machine code. Students may choose a networking problem to solve which might mean writing code that needs to communicate across the school's internal network.

Students may also choose to bring their own development system from home, for example a laptop with the relevant software for AS/A2 Level Computing, especially when working on their A Level project since they do a substantial amount of work outside of school. Students who bring their own systems into school would benefit from having sufficient access to the school's network so that they can access the Internet and access files from their home directory.

Students would also benefit from having access to a USB port to enable them to mount a memory stick and to connect to extension boards such as Arduino or .Net Gagdeteer.

[23] Details provided by Kevin Bond, Chair of Examiners for AQA AS/A Level Computing.

9 Appendix 2 – Case Study

9.1 Queen Elizabeth School, Cumbria

Queen Elizabeth School (QES), a 1400 pupil comprehensive in the market town of Kirkby Lonsdale, Cumbria has offered Computing at A-level for many years. More recently this has extended to GCSE options and KS3. Director of IT, Roger Davies teaches computing and oversees the work of the in-house technical support team. Technical support provides IT services to all subjects though the requirements of Computing provide most technical challenge. Having a structure that brings teaching and technical needs together means everyone can work to a common vision, with a shared understanding of the issues and risks.

The school allows unsupervised access to all IT facilities. This includes internet access and a variety of programming environments. Underpinning this 'relaxed' approach is a rigorous attitude to acceptable use founded on a belief that students must be actively involved in developing safe practices in school and beyond.

"We could try to prevent students from accessing a lot of things, but that would be counterproductive" argues Roger. "Technical solutions don't solve behavioural issues. Our prime concern is to educate students about the wired (and wireless) world they inhabit. A focus on restricting access, blocking and locking things down, puts technical support on a collision course with teachers and pupils."

Rights involve responsibilities. QES attempts to give pupils a framework, tools and support to deal with these responsibilities. This involves openness, an acceptance that students will make mistakes occasionally and positive encouragement to be honest when they do. That said, a supportive environment is only maintained because the school has robust procedures to quickly pick up problem behaviour as and when it arises.

Putting flesh on the bones of a policy requires a comprehensive pastoral programme engaging with the moral and ethical issues involved. "These are constantly changing," comments Roger, "In my experience, pupils welcome discussion and are willing participants. They always provide fascinating insights into the shifting trends in teenage behaviour. By encouraging debate, not only are you creating a climate of openness, but gaining a valuable window into their world at the same time."

Underpinning this approach is the provision of a network infrastructure that addresses three things:

- Keeping the network secure from external threats: configuring firewalls, maintaining up-to-date anti-virus software and keeping abreast of security patches;
- Implementing group policies that minimise the risk of accidental misuse; and
- Logging use and developing effective procedures for monitoring.

Four full time technical staff are led by Network Manager, Jim Williams. The school has financed training via Lancaster University and both Jim and his deputy, David Gradwell have completed degrees in Network and Systems Administration. Having skilled practitioners who understand a service provision role is central. They deal with a variety of teacher demands whilst managing a network of increasing complexity used predominantly by novices. Put that way, you can appreciate the concerns faced by those on the sharp end when things go wrong.

The specifics are less important than the principles on which change is agreed. This rests on good communication and dialogue. The team are at pains to understand teacher's requirements and take professional pride in developing innovative solutions. For example, A Level computing students can investigate networks, create shares, run a command line and implement packet sniffing, port scanning and other diagnostic utilities. This is possible through the provision of two networked Virtual Machines (configured with fixed IP addresses on a separate private range), residing on each pc in the computer suite.

10 Appendix 3 – Acceptable Use Policy

It is beyond the scope of this document to provide example acceptable use policies, however Becta identified good practice when writing an AUP as follows.

The AUP should:

- Be written by the school to ensure ownership and buy in rather than borrowed from elsewhere;
- Be clear and concise and ideally no more than two sides of A4;
- Reflect the school ethos, culture and values;
- Be produced in consultation with teachers, governors and pupils;
- Be written in a tone and style that is appropriate to the end-user;
- Promote positive uses of new and emerging technologies;
- Clearly outline acceptable and unacceptable behaviours when using technology and network resources provided by the school; and
- Use positive language.

When writing or reviewing the AUP for pupils or discussing what the AUP means there are some activities that can be referred to that may help them think about how they use technology. Some of these activities may have legitimate uses and may serve as useful exercises when teaching computer science courses and it's recommended that the ethics and legality of such activities are openly discussed.

Here are some suggested activities that could be referred to that would be considered unacceptable:

- The deliberate attempt to trick a fellow pupil or member of staff into revealing their password e.g. via a fake logon window or web page;
- The use of network traffic analysis tools to capture other users data without their consent;
- The installation of a DHCP, DNS, internet proxy or similar server services to capture other users' network traffic and redirect their connections;
- The deliberate by-passing of the school's internet filtering system or the provision of such a service to fellow pupils;
- The installation of remote access tools on school computers;
- The installation of covert monitoring or data capture tools on school computers including keyloggers;
- The deliberate introduction of malicious code into the school ICT system;
- The introduction of unapproved hardware devices onto the school ICT system;
- The introduction of wireless access points;
- Any attempt to steal or crack users' passwords;
- The unauthorised copying of data from the school ICT network;
- The downloading or sharing of copyrighted material;
- The unapproved use of computer games; and
- The installation or use of unapproved network based communication tools e.g. instant messaging clients.

11 Appendix 4 – Sources of Help and Advice

Computing At School

http://www.computingatschool.org.uk

Exam boards offering Computing or Computer Science GCSE and AS/A Level

OCR

http://www.ocr.org.uk/qualifications/by-subject/ict/ict-qualifications

WJEC-CBAC

http://www.wjec.co.uk/index.php?subject=212&level=15

Assessment and Qualifications Alliance

http://web.aqa.org.uk/qual/newgcses/ict/computer-science-overview.php

Microsoft

http://www.microsoft.com/education/en-gb/Pages/index.aspx

Google

http://www.google.co.uk/edu/index.html

RM

http://www.rm.com/home