

THE CAM ACADEMY TRUST INTERNAL IT DEPT POLICIES

To be read in conjunction with School Procurement Policies	
Approved in consultation with the Audit & Risk Committee on behalf of the Trust Board:	July 2018
To be reviewed:	Every two years or as appropriate
Date of next review:	July 2020
Responsible Officer:	P. Middleton; M. Norman
Category: 1	Version V1.0 V1.1 – Updated AUP Statement V1.2 – Added items about tender process V1.3 - Remove reference to The Voyager Academy

This document provides a set of policies for each school that joins The Cam Academy Trust to abide to. It puts into place a set of procedures to follow and acts as an instructional manual for IT departments across the trust to ensure the security of our data, cost effective working and protection of our users.

1.0 Procurement Policy

Each school shall have in place adequate procedures to ensure that all IT purchases are in accordance with authority limits, are aligned with the IT strategy and provide value for money. Local procedures should include the following items:

1.1 Budget

Authority levels should be in place to ensure that purchases are within authorised limits. Where the school has an IT Manager consultation with the Trust IT Manager is mandatory for software and hardware purchases greater than £1,000, where the school has no IT Manager then purchases over £200 should be passed through the Trust IT Manager and those under £200 should be in line with the budget set out for that individual school. Projects costing over £5,000 or where new software systems are being introduced should be automatically referred to the Trust IT Manager in the form of a project plan/proposal, so a review could be undertaken as to whether such platforms could or should be undertaken trust wide with the subsequent benefit of trust purchasing or indeed whether there was knowledge within the trust of the software/hardware being proposed.

1.2 Security Checked

Systems capability must meet the security needs of the Trust, i.e. system has password control functionality that conforms to the security policy, capable of restricting system access levels and maintains an audit trail.

1.3 Strategy Alignment

The purchase should be in line with the IT strategy for the trust and compatible with existing systems, with scope for enhancements.

1.4 Supplier Selection

Effective procedures should be in place to ensure that value for money is achieved.

1.5 Maintenance

All key equipment should be covered by a maintenance contract, although this may not be required for equipment that is easily/cheaply replaced. When maintenance contracts reach the end of their term, schools should consult with each other to investigate the possibility of obtaining Trust discounts by using the same supplier.

1.6 Quote Process

On orders over £1,000 three quotes must be sourced before a purchase is made.

On orders over £10,000 the following procedure must be followed.

- Planning phase must be started 12 months in advance of any major IT installation with contact with the Trust IT Manager from the start, initial indicative quotes should be received for budget purposes
- Three full quotes must be acquired using the Tender Process (See example in Appendix 1 (Page 8))
- A recommendation document (See Appendix 1 Page 8) should then be produced and sent to the governors for approval

2.0 Computer Security

2.1 Passwords

All schools must institute and maintain a system of alphanumeric password access and control that relates to the specific systems in operation. All trust schools must comply with the following minimum requirements:

- Minimum of 6 characters for students
- Minimum of 8 characters with 1 number and 1 special character for staff
- Must expire after 90 (ninety) days
- Password cannot be used again for 4 changes

2.2 System Access

No staff member should be given access to a School computer system by anyone other than the system administrator or by the automated Salamander system which will not arrange for such access unless he/she can confirm that the user is in the MIS system within that school. Staff should only be given access to areas of the network they will require. Students must not be given access to ANY areas of staff data.

Group policy must be in place to prevent students from being able to login to any admin\non student devices.

2.3 Logging

All logons (Staff and Students) must be logged in such a way as to allow the IT Manager to track who was logged onto a particular system at any given time, this information should be kept for a minimum of 1 full academic year (Sept to Sept).

2.4 Staff Obligations

All staff and students should be made aware of the Schools IT Policies and their obligations under them before they are allowed access (AUP). A message should be presented at login stating, this setting can be set using Group Policy:

By logging into this computer you accept that you have read, understood and agreed to the terms of the Acceptable Use Policy (AUP)

2.5 Employee Password Security

All staff should be aware of password procedures and be instructed that on no account should they disclose their password to any other person nor should they write it down. Whether allocated a password by the system administrator or forced by the system to choose their own, any suspected breach of their password security should be immediately reported to the IT Manager and their Head of Department.

2.6 System Security

To deny un-authorised access to the system by others when the authorised user is temporarily away from the screen, all computer screensavers should be password protected. It is permissible to utilise the current system password on the screensaver.

2.7 Password Protection Files

Where an individual user password protects sensitive school files on their computer and/or transmits protected files then only those to whom the files are being sent should know the password necessary to open the file. The sender should make a note of the password which should be kept in a sealed envelope preferably in the school safe. Unless the password is breached such passwords can remain unchanged.

2.8 Access Denial

HR/Personnel must notify the School IT Department immediately of any change in an individual's right of access e.g. leaving employment and such access logins must be disabled with immediate effect and a record kept of all such logins by the IT Manager.

2.9 Insurance

All security must meet insurance requirements and key equipment should be kept in a secure environment.

2.10 Domain Admin Account

Domain Administrator account user should not be used for login to ANY systems, user accounts should be used so audits can be taken as to when specific users have accessed servers etc, specific service accounts should be set up with complex passwords (8 characters, inc. alpha numeric and special), these passwords can be set to never expire but should never be used to log in, permission should also be given to the Domain Admin account in the event of this password being forgotten and these used for installed services, for example SQL Server should be installed and services created for use by a specific SQL user account (e.g. Sql.Admin).

Domain Administrator password should be changed at the end of every full term, the password should be written down by local IT Manager and stored in an envelope marked Domain Admin Password (Date) and filed in fire proof safe.

2.11 Encryption

All staff laptops and devices must have encryption enabled by default, we must assume the sensitive data may be stored on any staff device and as such must keep that data secure. The recommended solution to encryption is to have TPM chips in devices with Bit Locker enabled. Other Encryption software can be used but must be cleared by the Trust IT Manager.

All portable USB devices must be encrypted, a group policy must be put in place to block the usage of non-encrypted external storage devices which do not have encryption enabled on them for all staff.

2.12 External users

External users must only be connected to guest networks with no access to servers, there must be a guest VLAN in place so as to be able to restrict this access.

3.0 Office/Server Room Security

Sensitive information and expensive equipment is kept in IT Offices and Server Rooms, including computers and servers logged in with privileged accounts, IT staff must ensure that their screens are password locked when not in use and IT Offices and Server Rooms must be locked when nobody is in them

4.0 Anti-Virus Procedures

Antivirus software must be present on all points of entry, including connection to the network. Virus software should be updated at least on a weekly basis for PC systems and not, in any event, longer than a monthly basis for Apple Macintosh. In addition the following procedures should be adopted:

- 4.1 To help minimise the effects of viruses all staff must follow the policy set out in the schools AUP.
- 4.2 Each school will subscribe to the virus alert service of their Anti-Virus software supplier. Where a school becomes aware that their system has been infected, they will immediately notify all other CAT Schools of the infection and where known, the name of the virus. System administrators will immediately check any email traffic received from the infected centre and take remedial action where necessary.
- 4.3 No software, including anti-virus software, should be downloaded other than by the IT Team.

5.0 Staff Awareness

All staff and students should be aware of the school's Acceptable Use Policy and be made aware of the location of all IT policies. The use of the Internet and e-mail facility is primarily provided to a user as a school resource and in most circumstances should be limited to school use only. However, reasonable personal use is permitted where this does not interfere with an employee's normal duties. Reasonable in this context does not include the sending or downloading of material that might cause offence, however unintentional, to either colleagues or other individuals outside the trust.

6.0 IT Disaster Recovery/Business Continuity Planning

Each School will develop, test and implement an IT Disaster Recovery/Business Continuity Plan to ensure operational continuity in the event of a disaster. Such procedures shall be reviewed and signed off by the Governors on an annual basis. The plan will include:

- Identification of key school critical systems effected;
- Hardware and software requirements for the critical systems
- Redeployment of staff and hardware/software;
- Back-up procedures to ensure that software, data and documentation is recoverable in the event of corruption or failure of computer facilities;
- The acceptable timeframe for the effective recovery of systems, data or school processes to ensure operational continuity; data backups should be stored offsite;
- Contact details for all staff essential to the successful implementation of the BCP;
- Processes for periodic testing of the effectiveness of the BCP; and
- Procedures for public relations management (as necessary), including response by a person authorised to respond to any external enquiries relating to the nature of the incident and any potential liabilities that may occur.

7.0 Data Protection Act

All schools will abide by the Trust's Data Protection Policy.

8.0 Software Licenses

Schools should keep a record of all software used on each PC, together with a copy of the invoice, licence or proof of payment. These records should be held in a fire proof safe with a copy held off site. All schools must ensure that all software used throughout the school, including fonts, is legal and that the school has the correct number of licences for the number of users. All machines must be checked on a regular basis to ensure that no illegal software (including fonts) has been loaded.

9.0 E-mail/Internet

9.1 Internet Filtering

All Schools must have some form of internet filtering, recognised products for filtering include LightSpeed, WebSense and Sophos, there should be filtering of at least two levels, students and staff with Safe Search enabled for Students as a minimum

9.2 Disclaimer

Each school should put in place appropriate safeguards to protect and provide for corporate liability, system integrity and system availability.

Disclaimer:

Schools should use the following wording at the end of all external e-mails:

'This e-mail is confidential and may contain legally privileged information. If you are not named above as an addressee it may be unlawful for you to read, copy, distribute, disclose or otherwise use the information in this e-mail. Any views or opinions presented are solely those of the author and do not necessarily represent

those of (School name). If you are not the intended recipient and have received this e-mail in error, please notify (School name) on (telephone number).
Registered Office: (School name and address with Registered No.)

9.3 Student email

Students should be restricted from being able to send out to no more than 5 recipients at a time, they should be restricted from being able to send to any groups unless student related groups (For example student council etc), they should be restricted from being able to send to external contacts stored within the Global Address Lists

10.0 IT Equipment

- 10.1 All IT Equipment must be security marked in such a way that should the equipment be stolen or go missing it can be traced back to the school and identified.
- 10.2 All IT equipment, including but not limited to projectors, printers and computers must be stored in an approved list with at least information on, date of purchase, serial number, cost and location.

11.0 Mobile Devices Connected to School Resources

All mobile devices connected to school resources (For example email) must be protected with a minimum of a 4 number numeric PIN

Appendix 1: Example of Process to be followed (See para. 1-6 above)

Contents

Purpose	8
User Expectations	8
The Solution	8
Potential Problem Areas	8
Suppliers.....	8
ACS	9
Cambs ICT Service	9
BroadBerry	9
Conclusion.....	10
Appendix 1 – ACS	11
Appendix 2 – Cambs ICT Service	11
Appendix 3 – BoradBerry	12
Servers	12
Backup.....	13

Purpose

The trust has been working towards placing as many services as possible into the cloud to ensure not just resiliency but also to provide a platform for reducing the server requirements across the trust.

At present each secondary school must purchase servers every 5 years costing around £30 - £40k each time, this is not a sustainable model and merging schools into the trust should bring with it a saving on hardware costs at the same time.

At present each primary school runs on its own servers when they join the trust, these cost around £5 - £10k every 5 years, this cost can be completely subsumed into the trust solution.

It is proposed that a central server solution should be researched, proposed and implemented during the academic year 2017 – 2018.

User Expectations

Staff and students should be able to continue to work in the same manner they are accustomed to with no perceived change in service or performance, the solution being proposed should also alleviate the staffing situation in IT where at present it is required that a Senior Technician be present in each secondary school to support the server hardware.

The Solution

After many telephone conversations with various providers a solution that provides both resiliency and performance has now been fleshed out. The basic structure being proposed is this:

- A Microsoft Server 2016 Hyper-V solution (making management simpler than VMWare as it's known technology)
- Core servers hosted in two schools providing failover facilities should a major outage in one of the hosted schools occur
- Allow the servers to run in an 'active/active' mode allowing the full power of the system to be used always, but should an outage occur we can run the entire trust out of one school
- A backup (not active) being placed in a separate school to the core servers to act as a full off-site backup solution
- Physical Domain Controllers on each site so that internet, MIS and Email will continue to work even if one of the hosting schools goes down

Potential Problem Areas

There are a couple of areas in which this solution will potentially cause problems:

- If there is an outage in Comberton or Cambourne then the schools running out of that site will have no access to services provided by that site, for example, staff shares (unless hosted in SharePoint) will be unavailable. It is possible to spin these servers up in the other hosting site in the event of a prolonged outage thereby getting schools back up. A document will be produced during installation giving the circumstances by which we will make the decision to failover
- If a school plans to leave the trust they will be required to leave the trust IT solution and must provide their own hardware and migrate their data from trust systems to a solution of their choosing

Suppliers

We have approached three suppliers for this project:

ACS – ACS have already supplied wireless systems to Voyager and Comberton in the past and have shown great customer service, indeed they have also been approached to provide the wireless solution for the trust.

Cambs ICT Service – We have dealt with them in the past, although have not bought servers from them since Cambourne was opened, they have the best experience of supplying IT into schools but service from them can sometimes be poor.

Broadberry – A direct supplier of server hardware so cutting out the middleman, they provide hardware to the likes of Tesco, BBC, Google, Cambridge and Oxford University and NASA. The solutions have won countless awards over recent years.

We have requested a solution from each of the providers based on the requirements listed above, each solution fits the outlined purpose but is different based on what each provider sees as their solution.

ACS

ACS have proposed a solution which provides a run of the mill standard server SAN solution, my main concern with this solution is the complexity of management as we would need external 3rd party support for problems as it uses iSCSI. The solution also doesn't scale very well requiring a large investment should we need to grow

Their quote is under Appendix 1

Cambs ICT Service

The same requirement was sent to them but as of yet (3 weeks of chasing) they have not sent me a quote, sadly this has become standard practice for them and makes me reluctant to use them for the project due to poor pre-sales and after sales service, I suspect we will not be using them again in the future.

Their solution from the phone calls would be a DELL VRTX solution, this is a kind of hybrid SAN Server solution that could provide

Should their quote arrive it will be in Appendix 2

BroadBerry

The Broadberry solution works on the same basis as most data centre solutions do now (HyperConverged), that is a simple server only based solution where 2 servers are linked together to provide a simple yet powerful single server solution across two sites to offer resiliency, this offer simple support, quick installation, great resiliency and massive scalability.

Quote is in Appendix 3

Supplier	Manufacturer	Cost
ACS	Dell	£78,607.00 Exc Backup
Cams ICT Service	Dell VRTX	Unknown
Broadberry	Broadberry	£80,016.61 Inc Backup

Conclusion

We have discussed with each supplier the benefits of each solution, the ACS is a familiar solution that has worked in the past but with external support required to be added to the cost, this increases the cost of the solution massively making it beyond our reach. That said I believe that technology has moved on over the last 5 years and this Server/SAN technology is being phased out.

Cambs ICT Service have once again let us down in not providing a quote in a timely fashion, the solution being proposed from initial conversations looks good, but I have concerns over resiliency, we'd essentially be 'putting all our eggs in one server sized basket', any hardware failure on that one server would mean all schools having no access.

BroadBerry have provided a future proofed solution, it provides more than enough CPU, RAM and Storage to support the trust over the next 5 years and leaves us room to grow, they have also managed to provide a backup solution into the cost as well as we are able to go direct to the manufacturer and thereby cutting out the 3rd parties on costs.





The brief was to have a solution that was easy to manage, simple to install, easy to maintain, great resiliency and expandable should it be needed.

While we are looking to move to the cloud over the coming years we need a solution that can grow easily if the move to the cloud proves to be an incorrect approach, this solution offers us the facility to grow the solution without too much expense.

I recommend we go with the solution provided by BroadBerry, pound for pound they are offering more performance and better resiliency than the other two solutions.

Appendix 1 – ACS

acs

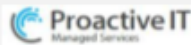
Quote Ref: QUO-226671-1

Client: CAT (Comberton / Cambourne Village Colleges)

Client Contact: Paul Middleton

Quote Date: 23.03.2018

Quote Expiry: 22.04.2018

Description - 50TB Useable	Part Code	Qty	Price	Cumulative Price
Server Hosts				
Dell PowerEdge R640 2 x Intel Xeon Silver 4110 2.1Ghz 8C/16T 9.6GTs 11M Cache Turbo HT 96GB RAM RDIMM Dual Rank 2880MT/s iDRAC 9 Enterprise 2 x 120Gb SSD SATA Boot Drives PERC H730P RAID 2GB NV Cache 2 x 750W Redundant Power Supplies Broadcom Quad Port 1000T NIC x2 Broadcom 57416 Dual Port 10Gb BaseT 5 Year ProSupport Plus 4 Hour Mission Critical	102809925/2	6	£8,268.50	£37,611.00
SAN				
Dell Compellent SCv3000 Dual Controller Array 8 x 1.92TB SAS 12Gb RI SSD, 14 x SC 4TB SAS 12Gb 7.2K 3.5", 10GB iSCSI 4 Port Copper Redundant Power Storage Centre Core Software base licence 5 Year ProSupport Plus 4 Hour Mission Critical	102810066/2	1	£29,448.00	£29,448.00
Switching				
Dell Networking N4032 24 x 10GBASE-T 2 x AC PSU Dell 5 Year Pro Support NBD On Site	102809925/2	2	£5,774.00	£11,548.00
Total excluding VAT			£78,607.00	
CABLES excluded unless otherwise stated				
<div> <div>Prepared by acs Pre-Sales Sarah Muse 07795 976323</div> <div>sarahm@acs365.co.uk</div> </div> <div> <div>  <div> <div>To learn more about how Proactive IT from acs could benefit your business please contact us today.</div> <div>www.pic365.co.uk</div> </div> </div> </div> <div>acs Terms and Conditions available on request</div>				

Appendix 2 – Cambs ICT Service

Still awaiting a quote.

Appendix 3 – BroadBerry

Servers



CyberStore 208-4N 12Gb/s SAS with 4 x NVMe Drive Bays - Performance Storage



- Up to 2x Intel Xeon Scalable Processors
- Up to 24 DDR4 ECC Registered Memory Slots
- Up to 8x Hard Drives
- HBA - 4i and 4 Port Port LSI HBA Controllers (Non RAID) and LSI RAID Controllers (Hardware RAID levels 0, 1, 5, 6, 10, 50, and 60) Raid Card
- Supports 4x Intel 40GbE Ethernet Adapters, Fibre Channel Adaptors, Intel 10GbE Ethernet Adapters and Gigabit Ethernet Adapters PCI Express Expansion
- Stores up to 64TB of data

Qty	Description
4	CyberStore 208-4N 12Gb/s SAS with 4 x NVMe Drive Bays - Performance Storage
	Supermicro SuperServer 6029UZ-TR4+
	2x Intel Xeon Gold 6148 Processor - 20 Cores, 2.40GHz, 27.5MB Cache (150Watt)
	10x 32GB 2400MHz DDR4 ECC Registered DIMM Module
	LSI 9300-4i Host Bus Adaptor (Non RAID) - 12Gb/s SAS 3.0 - IT mode
	2x 480GB Intel SSD 54500 DataCentre SERIES 2.5IN SATA3 TLC (OS)
	8x 6TB Enterprise Class SAS3 12Gb/s 7200RPM - 3.5"
	Mellanox ConnectX-4 EN NIC, 40GbE dual-port SFP, PCIe3.0 x8 with RDMA Ethernet Adapter
	2x Intel P4600 1.6TB Drive - 2.5 nVME - 560k IOPS Read, 177k IOPS Write
	Mellanox 40 GbE QSFP cable MCP2M00-A00A 1m (redundant point-to-point interconnect for S2D node communication)
	MIRRORED CONFIGURATION 42TB USABLE
	Rear caddies for OS drives
	10GbE Dual-Port RJ45 Server Adapter - Intel X540T2
	TPM 2.0 - Trusted Platform Module with TCG 2.0
	3 Year On-Site Warranty
	9-5 Technical Support for System Lifetime
	48 Hour Comprehensive System Testing Procedure
	UK Country Kit & Mains Cable
System Price: £18,868.19	
Total: £75,472.76	

Backup



CyberServe XE3-208S v6 - Backup server



- Supports up to 8x SATA2 and SAS Hard Drives
- Powered By 1 Intel Processors
- Supports up to 4 modules of DDR4 ECC Unregistered Memory
- 2x PCI Express Expansion Slots
- Configurable with up to 64GB Server Memory

Qty	Description
1	CyberServe XE3-208S v6 - Backup server
	2U Chassis with 8 Hot Swap Drive Bays & 2 Internal Fixed Drive Bays - Single 560 Watt Power Supply
	X115SL-F with DUAL Intel Gigabit LAN & Dedicated LAN for IPMI & Remote KVM Management
	Xeon E3 1220 v6 Quad-Core 3.0GHz 8Mb Cache 8GT/s 80Watts
	2x 8GB 2400MHz DDR4 ECC Registered DIMM Module
	LSI MegaRAID 9361-8i 12Gb/s SAS/SATA RAID Controller, 1Gb DDR4 Cache
	2x 240GB Intel SSD 54500 DataCentre SERIES 2.5IN SATA3 TLC (Onboard RAID 1) - fixed internally
	8x 10TB Enterprise Class SAS3 12Gb/s 7200RPM - 3.5" (RAID 6) - >50TB Usable
	RAID Controller Zero Maintenance Flash Cache Protection
	3 Year On-Site Warranty
	9-5 Technical Support for System Lifetime
	48 Hour Comprehensive System Testing Procedure
	UK Country Kit & Mains Cable
System Price: £4,484.05	
Total: £4,484.05	



**BEST PRICE
GUARANTEED**

We won't be beaten on price! We're so confident in our fantastic value, we guarantee you won't find the same spec at this price elsewhere!

Sub-Total	£79,956.81
Carriage	£60.00
Credit Card Surcharge	0%
Nett Total	£80,016.81
VAT Total (20%)	£16,003.36
Gross Total	£96,020.17