

Honiton Community College Academy Trust



This Policy was adopted by the Governing Body of
Honiton Community College Academy Trust
on 7th December 2016
and will be reviewed every 2 years.

ICT POLICY

ICT Policies Contents

Introduction and Overview	4
Acceptable ICT use for Students	5
Policy	5
Procedures	6
Acceptable ICT use for Staff	6
Policy	6
Procedure	8
E Mail Policy	8
External Access	9
Software Purchasing	9
Hardware Purchasing	9
Loan Equipment	10
Fault Request	10
Password Policy	10
Students Passwords	10
Staff Passwords	11
Username Policy	11
Students Policy	11
Access Accounts	11
Network Security Policy	12
File Management Policy	12
Shared Documents	12
Inappropriate Use policy	13
Facility Booking Policy	14
Network Room Booking	14
ICT Support Requirements	14
User Access Policy	14
College Network	14
SIMS	15
SIMS Remote Access	15
College Virtual Learning Environment	15
E-Portfolio Access	15
E-Mail	16
Disaster Recovery Policy	16
Data Backup Policy	16
SIMS MIS server	16
Connect3 Network Servers	16
Staff Laptops	17
ICT Budgets	17
Personal Laptop Internet Provision	17
Social Networking Sites	17
Appendices	19
Appendix A: Student Email Account Access by Staff	19
Appendix B: Network Email Account Setup Form	20

Appendix C: Staff Network Account Access Form	21
Appendix D: File Restore Request Form.	22
Appendix E: Internet Filter Release Form	23
Appendix F: Current Service Contracts	25
Appendix G: Internet Access Application Form:	26
Appendix H: SIMS Remote Access Form:	28
Appendix I: Social Networking Use Application Form	29
Bring Your Own Device Policy.....	31
Document Change History.....	34

Introduction and Overview

The use of ICT is essential for the curriculum delivery and the college administration. All staff and students will make significant use of ICT whilst engaging in college activities. This policy documents lays out the principles and outline procedures which allow for the efficient and safe management of our facilities.

At all times both, Child Protection law and polices, with the Teaching Standards and The Pay and Conditions documents will have precedent over this Policy. The document will not provide protection to staff or students whose use of ICT contravenes any other polices or nationally recognised agreements. All staff and students are responsible for their own actions when using ICT and Computing systems at Honiton Community College.

This policy also considers our obligations under ICT Law in particular the following areas of Legislation;

- Data Protection Legislation
- Computer Misuse Legislation
- Copyright Designs and Patents Legislation
- Health and Safety Legislation

Whilst every attempt has been made to include sufficient detail of all our polices and procedures the complexity of our network and the variety of tasks carried out using it may require additional procedures to be followed which are not detailed in this policy. Staff and students will be informed of these at the appropriate time.

If there are any changes in legislation, national guidance or college policy we will change the policies and procedures accordingly. Staff will be informed with sufficient notice and ELT approval will be sort

Acceptable ICT use for Students

Students and parents/guardians need to be clear as to the student's responsibilities when using college ICT equipment. We have created a clear acceptable use policy for students to follow.

Policy

As a student at Honiton Community College you have access to a wide range of ICT hardware and software. The information age gives you access to a large amount of information and methods for manipulating it which will help you with your learning. However there are a few straight forward rules which we need you to follow to ensure our facilities are **cared** for and you are **safe** whilst using them.

Passwords

- ✓ I will always logon with my *own* username and password.
- ✓ I will keep my password *safe* and *secure*.

Network Area

- ✓ I will keep my documents area *organised*.
- ✓ I will *remove* files which are not required (e.g. pictures files in another piece of work).

Computer Use

- ✓ I will ensure that all files brought in or sent to school have been scanned for *viruses*.
- ✓ I will use *authorised* software only on school equipment.
- ✓ I will *care* for the computer equipment and ICT facilities.
- ✓ I will only *print* work for school.

Internet Access

- ✓ I will only access the internet when *requested*.
- ✓ I will only access sites *relevant* to my projects.
- ✓ I will inform the teacher if I find *inappropriate* material.

E-Mail Use

- ✓ I will use e-mail sensibly.
- ✓ My e-mails will always be polite.
- ✓ I will ensure my e-mails are sent to people expecting them.
- ✓ I will inform my teacher if I have received:
 - Inappropriate e-mails.
 - E-mails which are threatening.
 - E-mails with bad language.

VLE/E-Portfolio/Social Network Sites

- ✓ I will use all VLE/E-Portfolio /Social Networking Site features **responsibly**.
- ✓ I will use appropriate **language**.
- ✓ I will use appropriate **Images**.
- ✓ I will set and maintain **secure security settings**

- ✓ I will keep my **personal details** private and be aware of my digital footprint
- ✓ I will respect people's **privacy**;
 - By asking their permission before I use their name or image
 - By considering their feelings first.
- ✓ I will respect peoples different **points of view**;
 - By stating my viewpoint politely
- ✓ I will inform my teacher or a responsible adult if I find;
 - **Inappropriate** content or links to inappropriate content.
 - **Offensive** use of the VLE/E-Portfolio /Social Networking Site
 - **Cyber-bullying** of my self or another student.

Access to the school ICT facilities is a privilege. We will use our tracking facilities to ensure that the ICT facilities are being used appropriately. If we find that these rules have been broken then we will remove your ICT privileges and inform your head of learning or senior member of staff.

I have read and understand the ICT appropriate use policy:

Procedures

To ensure all Students and parents/guardians are aware of the policy the following will be implemented.

- A copy of the policy will be published on the College Website
- All Students will be required to electronically acknowledge the College AUP Policy every 90 days when logging into the college network
- ICT Teachers will discuss the policy at the beginning of each year showing pupils the document on the College Website.
- When new users are given access to the Network, technicians will remind them of the ICT Support policy.
- During the year Students will be reminded of the policy at appropriate intervals.
- If a student does not follow the College Acceptable Use Policy then the procedures in the unacceptable use section will be followed.

Acceptable ICT use for Staff

So staff are aware of their responsibilities they will need to know the appropriate use of the College's ICT facilities.

Policy

As a member of Staff at Honiton Community College you have access to a wide range of ICT hardware and software for your professional use. There are a few straight forward procedures which we need you to follow to ensure our facilities used professionally and safely.

Policies

- ✓ Current relevant ICT policies and procedures will be followed.

Passwords

- ✓ Logons will only take place with the appropriate username and password.
- ✓ Passwords will be *secure*
- ✓ Full responsibility will be accepted for actions taken when using your credentials.

Network Area

- ✓ Home directory areas will be *organised*.
- ✓ Unnecessary files will be *removed* from the network (e.g. pictures files in another piece of work, personal files not related to professional duties).

Computer Use

- ✓ Will be professionally appropriate at all times.
- ✓ *Laptop Virus protection will be updated via the internet weekly.*
- ✓ All files brought in or sent to College should be scanned for *viruses*.
- ✓ *Authorised* software should only be used on College equipment.
- ✓ Computer equipment and ICT facilities will be cared for.
- ✓ *Printed* work should be for professional use only and kept to a minimum.
- ✓ All issued ICT equipment must be returned when employment with the college terminates.

Internet Access

- ✓ Will be professionally appropriate at all times.
- ✓ Any unfiltered inappropriate websites known to staff should be informed to ICT support in accordance with the college website filtering policy.

E-Mail Use

- ✓ E-mails will be checked daily during college
- ✓ E-mails will always be polite.
- ✓ E-mails are sent to appropriate recipients only.
- ✓ An appropriate member of Management will be informed if any of the following occurs;
 - E-mails which are inappropriate.
 - E-mails which are threatening.
 - E-mails with bad language.
- ✓ Inbox and folders will be managed effectively.

Website Use

- ✓ Only approved staff will update the College website
- ✓ Only approved material will be submitted to the website
- ✓ All copyright laws will be followed in terms of resources and appropriate levels of security.
- ✓ Student photographs/images will not be identifiable by name for those students who have not consented on the data collection survey form.

Data Protection

- ✓ Professional information and data will be kept secure
- ✓ Confidential information outside of SIMS will be **encrypted**
- ✓ Professional information and data will not be forwarded to an outside person/organisation unless authorised by senior management

- ✓ Only current, relevant and accurate data will be stored.
- ✓ Current legislation will be implemented at all times unless directed otherwise by a senior member of staff.

ICT use with Students

- ✓ Students will be expected to follow the students ICT appropriate use policy
- ✓ Facilities will be booked following the current procedures
- ✓ Facilities and equipment will be cared for in a professional manor
- ✓ Student will be asked to tidy the ICT stations appropriately

VLE/E-Portfolio/Social Network Sites

- ✓ VLE/E-Portfolio /Social Networking Sites will be used **professionally**
- ✓ **Secure Security settings will be set and** maintained regularly
- ✓ Procedures and the Terms and Conditions for Social Networking Sites will be adhered to.
- ✓ All files, images and text will have appropriate **security** settings and adhere to copyright agreements

The use of all College ICT equipment and facilities is necessary for effective fulfilment of professional duties therefore contravening the appropriate ICT use policy could result in disciplinary procedures in accordance with College policy and may result in dismissal.

Procedures

To ensure all Staff are aware of the policy the following will be implemented.

- A copy of the policy will be published for staff only on the College website.
- All staff will be inducted for the ICT acceptable use policy.
- During the year staff will be reminded of the policy at appropriate intervals
- Appropriate senior management will be informed of any breaches of the acceptable use policy.
- Changes to policy will be communicated to all staff immediately.

E Mail Policy

To allow effective communication the whole college community will have access to a personal e-mail address.

The current provider of our e-mail services is Microsoft Live and they provide a web based e-mail service which can be accessed from any computer with internet access at the following address;

<https://login.live.com/>

Access will be via password and username in accordance with the College ICT password policy.

E-mail use will be in accordance with both staff and student acceptable policies.

10GB of user storage space is provided and staff/students are expected to manage this provision effectively.

Inappropriate language is filtered, including coded references to inappropriate words and the e-mail is returned to sender and not forward to the recipient.

Staff will be expected to check their E-mails daily and is considered a primary form of communication in the College.

External Access

KS3 and 4 Students don't have access to external e-mail address outside of the honitoncollege.devon.sch.uk domain.

KS 5 Students do have access to external e-mail addresses outside the college domain.

If staff require students to have different access requirements the form E-Mail Permissions must be completed.

Software Purchasing

Software to be considered for purchasing for use on College ICT Network facilities needs to be approved as acceptable. Testing and approval can be arranged via the network manager.

All commercial licensing agreements should be followed.

Master Lists of all software purchased and licences bought will be held on College Software list.

All master discs and licences will be held by ICT Support and kept securely.

Hardware Purchasing

Hardware to be considered for purchasing for use on College ICT Network facilities needs to be approved as acceptable. Testing and approval can be arranged via the network manager.

Master inventory of all hardware purchased will be held by the network manager and all ICT purchases will be recorded in the appropriate section.

All master discs will be held by ICT Support and kept securely.

No equipment should be connected to the College ICT network facilities without approval from ICT Support via the network manager.

Loan Equipment

The College may provide ICT equipment for staff or students use. A signature will be required for all high value items and the completion of a loan form for long term equipment loans.

All loaned equipment should be kept securely and safely at all times. Staff will be responsible for claiming on their personal home insurance for damage or loss when in their personal possession out of college. Staff should **not** leave loaned equipment in an unsupervised car as many insurance polices will not pay a claim. Staff will be expected to cover the full value for an item lost in this way.

Any lost, stolen or damaged equipment may be chargeable at the discretion of ELT. The value will consider the age of the equipment and the technical support time to remedy the damage.

Fault Request

All errors or faults need to be communicated to ICT support as soon as possible using ictsupport@hontioncollege.devon.sch.uk. Requests will then be prioritised and dealt with as soon as possible and staff will be informed when complete. This is managed by the network manager who allocates support calls according to staff availability and College requirements.

Fault requests will be analysed to help with budgeting, staff training and ICT development planning.

Password Policy

The following guidelines should be followed when users are asked to create a password.

Students Passwords

All students will have a unique password. Their password must:

- ✓ Have letters and numbers
- ✓ Not be easily guessable

- ✓ Must be easily remembered
- ✓ Must be kept secure
- ✓ Must inform ICT support if they suspect someone knows their password

Staff Passwords

All Staff will have a unique password. Their password must:

- ✓ Have letters and numbers
- ✓ Not be easily guessable
- ✓ Must be easily remembered
- ✓ Must be kept secure
- ✓ Must inform ICT support if they suspect someone knows their password

Username Policy

Students Policy

1st name and Surname joined together with no spaces. Duplicates will then become identified with a letter after the name. E.G johnsmitha, johnsmithb.

Website logons have HCC_ prefixed to their username.

NB; Students who joined the college before September 2006 have their network username as the year they joined in two digit format, plus the 1st four digits of their surname followed by the 1st 2 digits of their 1st name. EG: John Smith who joined in 2003 will be '03smitjo'.

New student users who begin during the academic year will be notified to the ICT support staff by existing procedures. ICT support staff will be allocated to amend records and create new users in accordance with the ICT policy.

Access Accounts

The following accounts for each user will be created at the appropriate user level.

Students

- Network
- Website/VLE
- E-mail
- Sam Learning

Staff

- Network
- Website
- E-mail
- Sam Learning

- SIMS

Parents

- HCC Learning Gateway
- Parent Mail
- Parent Pay

These accounts will be created for all users when they start with Honiton Community College at the beginning of the academic year. When staff users start during the year a **new user form** (see appendices) should be completed and authorised by a head of department or senior manager of the college.

Network Security Policy

Best practice procedures are followed with regard to Network Security. This includes the following

- Virus Checking – All PCs and Network Devices will have virus checking
- Internet provision provided by South West Grid for Learning
- Firewalls incorporated and managed by Southwest Grid for Learning
- Authorised Users given access only with username and password
- User training on Security and appropriate polices given
- Physical Security is implemented where appropriate
- Data backed up regularly in accordance with backup policy
- Server rooms/storage kept secure at all times
- Web filtering internally and externally (SWGFL) monitored regularly
- Wireless access points all follow WEP Encryption and MAC address filtering

File Management Policy

All files need to be stored in accordance with the file management policy. Each user will be given appropriate read write access to the relevant network area.

Shared Documents

Only network administrators can create folders in Shared Documents and College Admin. The owner of each folder will be recorded on the Folder Owner List and they will be responsible for the management of their folders and sub folders.

Each Folder manager in consultation with ICT support will develop their own File management policy stating who has access rights to the network space. This policy will be included in curriculum/college documentation.

Inappropriate Use policy

Inappropriate use will be constantly monitored for using a range of facilities from the list below.

- Internet Auditing
- File Scanning (network and laptops)
- Use Logs
- E-Mail Auditing
- Staff Comments
- Student Comments
- Social Networking Sites Monitoring

ICT support staff will regularly check student/staff account areas for misuse. The record of searches will be logged and can be accessed by Senior Management.

Any Student ICT users who breach the 'Acceptable use policy' (AUP) should have the event recorded using existing college procedures via the **cause for concern slips**. This allows a record to be stored on SIMS. Breaches will be logged under the following heading – Breach of ICT AUP and the reason for the breach.

Teachers and ICT support staff are encouraged to discuss the student's breach of the acceptable use policy and discuss the consequences and why the college has to enforce the rules. Students will be asked to reread the AUP before being given access again. For regular or serious breaches of the AUP the Director of ICT, with the appropriate head of learning, may request a meeting with the students parents/careers to discuss matters further.

Students who seriously breach the acceptable use policy will be immediately disabled from all ICT facilities and the appropriate HoL will be informed to decide suitable action.

Staff who breach the acceptable use policy will be informed of their breach and offered additional training if necessary. However for a serious breach where staff actions may be classed as misconduct then an appropriate member of senior management team will be informed.

Note:

1. South West Grid For Learning constantly monitor internet usage and will inform the appropriate authorities of inappropriate internet activity.
2. ICT support use the following tracking facilities to ensure appropriate use of College ICT equipment. Access to staff accounts will be by requests from ELT and will be in writing. The ELT member or HoL will be requested to witness this access and a record will be kept using 'ICT access form'.

- Internet Auditing
- File Scanning (network and laptops)

- Use Logs
- E-Mail Auditing

Facility Booking Policy

Network Room Booking

ICT rooms booked in advance using our Live booking system as part of the room feature when creating calendar events.

Online tutorials and guidance notes are available on the ICT support section of the VLE.

Rooms may be booked outside of this agreement with prior arrangement from the facilities manager and relevant SLT approval.

Outside of college hours infrastructure use must be booked via the Network Manager in advance to avoid planned networked maintenance.

Other ICT facilities should be booked in accordance with College letting arrangements policy.

ICT Support Requirements

Any planned additional ICT requirements must be booked via the Network Manager at least a week in advance to allow appropriate levels of support to be made available. This should be recorded in the ICT **master diary** held in the ICT support office.

User Access Policy

All levels of user access will be defined and users recorded in the User Access log. Changes will only be authorised by the network manager or SMT member with appropriate understanding and responsibilities.

College Network

The college network is a RM Connect 3 network running over 4 servers with an Ethernet backbone connected to SWGFL internet service. It is a secure network which requires a user name and password. We follow recommended profiles sets in line with system specifications.

Access Level	College Users
Administrator	ICT support Staff only

Advanced Staff	ICT Teaching Staff
Staff	Standard Teacher Account
Advanced Student	Students who need Macro Access
Student	College Students

SIMS

SIMS is the college management information system (MIS) and is the primary system for college administration. There are 36 different levels of access depending on roles and responsibilities. ELT will decide user access requirements in consultation with System manager.

SIMS Remote Access

Using SCOMIS terminal services SIMS can be accessed remotely using commercial standard security internet access (VPN – Virtual Private Network). This access will be authorised by ELT for appropriate staff. Staff will complete the 'SIMS Remote Access form' which includes the conditions of use reminding staff of their responsibilities.

College Virtual Learning Environment

The college Virtual Learning Environment is hosted by UniServity and has a direct link from the college URL www.honitoncollge.devon.sch.uk. The VLE allows for extended learning opportunity for the whole learning community.

Staff access and user profile sets are controlled by the system administrators.

Access Level	College Users
System Administrator	Network Manager Head of ICT
Master Editor	Shelagh Andrews
Subject Department Owner	Respective HoD
Department Editors	Respective Members of Department
Year Group Owner	Respective HoL
Staff	All Members of Staff
Teachers	All teaching Staff
Governors	All Governors
Students	All Students in year group profiles

E-Portfolio Access

The College VLE has the facility for Staff and Students to create their own E-Portfolio. This e-portfolio facility will be given to all College members. Students are asked to use the facility responsibly and this is stipulated in the student AUP. The facility may be withdrawn by appropriate college management. Staff are expected to use the facility in accordance with their professional duties and responsibilities.

E-Mail

E-mail is delivered using Microsoft Live web based services. We follow recommended profiles sets in line with system specifications.

Access Level	College Users
Manager	ICT Support Staff
Password Changer	ICT Support Staff ICT Teachers
Staff	All College Staff
Students	All College Students

Disaster Recovery Policy

The network manager is responsible for producing the **Disaster recovery documentation** which is held in the safe and updated with critical information when necessary.

The documentation allows for full system recovery by providing critical settings and emergency contact numbers. Outline emergency procedures are included to aid recovery.

All network support staff are briefed and made aware of current disaster recovery procedures and updated when necessary.

Data Backup Policy

To protect the files stored on the college network from malicious or accidental damage or deletions the college has a comprehensive data back up policy. For files which have been deleted users can request an install by completing the File Restore Request Form.

SIMS MIS server

Remote back up provided by SCOMIS stored at Great Moor House and mirrored to County Hall. Daily back up with full restore options for up to 3 months. This is an annual contract.

Connect3 Network Servers

Remote county backup as above.

Staff Laptops

Staff can be synchronised with the college network for storage of college related data files. The responsibility for laptop backup rests with staff who should consult ICT support staff for the most appropriate method.

ICT Budgets

The ICT budgets receive an annual budget and are controlled by the Network Manager in consultation with Director of ICT. See appendices for current annual support contracts.

Personal Laptop Internet Provision

Students who need access to college internet facilities will need to be aware of the terms and conditions as detailed on the application form (appendices G). These conditions highlight the important rights and responsibilities of appropriate internet access. The student will have to obtain permission from their head of learning and their parents or carer before access will be given.

All internet access is monitored by educational ISP providers and any inappropriate or illegal use is reported to the relevant authorities.

ICT support will keep copies of the applications forms and record all technical details as required in the ICT support technical documentation to allow monitored access.

This provision may be withdrawn at any time due to technical reasons or to allow an investigation into inappropriate use. Any inappropriate use will be reported to the heads of learning or ELT member.

Social Networking Sites

Technology is a vital part of Educational success and in recent years the use of Social Network Sites has significantly increased and become part of main stream culture. Honiton Community College will allow staff and students to explore these sites safely and to develop the appropriate attitudes and skills required of the 21st century. We aim to investigate and develop suitable approaches to the use of Social Networking Sites with the following procedures and terms and conditions.

Procedures

- Any Social Networking Site use will require ELT Approval

- A Social Networking Use Application Form will be submitted to the Director of ICT
- The Network Manager will create the primary account and securely store the username and passwords with other key passwords. These will be provided to appropriate staff.
- All staff and students will be provided with appropriate training and advice with particular reference to protecting their public/professional reputations and a detailed understanding of appropriate security settings.
- All Social Networking use will be inline with the College ICT AUP
- All participants have the right to have posts/uploads/images concerning them removed if required.
- All participants are aware of our E-safety Guidelines. These are embedded in our acceptable use policy and shared on the college website, discussed in lessons and assemblies for students and covered during training for staff.

Terms and Conditions:

- All Social Networking Sites use should be reasonable and appropriate for college purposes
- All use of Social Networking Sites will comply with current legislation.
- Regular checks of appropriate use must be carried out
- Your login details are to be kept secure and only used by the registered account holder.
- You are personally responsible for all posts, access and updates with your login details
- Any posts which are deemed inappropriate by the College must be removed immediately
- The College retains the right to close/amend/delete any accounts without notice.
- Misuse of Social Media Sites may initiate college disciplinary procedures.

Private Use of Social Networking Sites:

- Security settings should be reviewed and appropriately set to ensure the College is not bought into disrepute.
- Staff must use professional accounts when using social network sites for College activities.
- College Confidential information must never be shared on Social Network Sites
- Any child safeguarding incidents must be reported to the designated child protection officer in line with College Child Protection Policies.

Student Email Account Access by Staff



The following Student's email account is to be accessed by the member of Staff listed below. Only the Network Manager can authorise this request and will be present during any investigation / inquiry. Once the investigation is complete the account password will be changed by the Network Manager.

Student Name	Tutor Group

Member of staff's name.....

Signature.....

Date.....

The account above was accessed by me for the following reason:

ICT Support Notes:

Appendix B: Network Email Account Setup Form

Network / Email Account Setup Form



This form is to be used by any new member of staff (Admin or Teaching) to request the setup of an ICT Facilities for the Honiton Community College Network. The form will need to be counter signed by the new member of staff's head of department.

First Name	Family Name
Department	Position
Start Date	End Date (if known)

Requirements (Please Tick) Network Email Website SIMS

New User

I confirm I need access to the above ICT facilities to carry out my appointed duties and I have read and will follow the College ICT policy.

Signature _____

Print Name _____

Date _____

Head of department

I confirm the person named above is a new member of staff and requires the above accounts.

Signature _____

Print Name _____

Date _____

ICT Support staff

The above account was created with the following details:

Username

Admin/Curriculum (delete)

Date

Staff Network Account Access



By signing this form you are requesting access to a member of staff's individual network account and all the data within it, which remains the property of Honiton Community College.

Only a member of the Senior Leadership Team is authorised to make this request and only the Network manager can grant the request.

Account to be accessed:

Name of ELT member:

Signature of ELT member:

Date:

Network Manager's name:

Network Manager's signature:

File Restore Request Form



Date		Time	
------	--	------	--

Name of Student or Teacher		Username	
----------------------------	--	----------	--

Name of file or folder to be restored			
---------------------------------------	--	--	--

Location of file or folder			
----------------------------	--	--	--

Result			
--------	--	--	--

Internet Filter Release Form



This information may be provided by E-mail.

Date required.....

Start time.....

End time.....

Full website address.....

Please ensure you have the full Internet website address you require to be released.

Today's date.....

Name.....

Dept.....

Signature.....

Current College Software Licences



2D Design
Acrobat reader 6
Advanced Biology
Advanced Physics
AQA Mathematics
Autograph
Circus Maths
Crocodile Chemistry
Crocodile Technology
Crocodile ICT
Crocodile science
Serif Drawplus 7
Serif Drawplus 8
Serif Pageplus 8
Serif Pageplus 11
Serif Photoplus 9
Serif Movieplus 5
Serif Photoplus 11
Serif Webplus 10
Stelarium
Edexcel Maths
Flowol 2
Food in focus
Geometry 11 plus
GCSE Science
Inspiration 7
Interactive food facts
Macromedia Studio MX 2004
Metro electro
Mission maker
MS Office 2003
MS Publisher 2002
Nessy
Number Shark
Omnigraph
Open Office
Prodesktop
MS Publisher 2003
Touchtype
Viewpoint 1.0

Appendices F: Current Service Contracts

Contract Description	Cost PA
RM SafetyNet Universal SECONDARY for RMSC2 Renewal	£299.00
RM SmartCache 2 Support (R)	£101.00
RM Virus Protect CC3 C2 - 100 Licences 1YR Renewal	£245.00
RM Virus Protect CC3 C2 - 100 Licences 1YR Renewal	£245.00
ServerCare Next Day On-Site (R)	£450.00
ServerCare Next Day On-Site (R)	£450.00
ServerCare Next Day On-Site (R)	£450.00
SWGfL 8Mbps Qtly, ref Honiton Communit-35314-11	£6,850.00
SWGfL Mail 100 Mailbox Renewal Quarterly	£94.00
SWGfL Mail 100 Mailbox Renewal Quarterly	£94.00
SWGfL Mail 30 Mailbox Renewal Quarterly	£28.20
SWGfL Mail 30 Mail box + Calendar Managed Service Qtly	£51.20
SWGfL Mail 40 Mailbox Renewal Quarterly	£39.60
SWGfL Mail 400 Mailbox Renewal Quarterly	£540.00
SWGfL Mail Bundle 500 Mailbox+1GB Renewal Quarterly	£470.00
Uniservity: Annual Licence with E-Portfolio (E-learning Credits)	£5400
SAM Learning (E-Learning Credits)	£3495

Use of College Internet Access for Personal Student Laptops



Application Form:

The college can provide you with wireless access to the college internet facilities for educational use.

You will need to read the terms and conditions of this service and if you agree to them please complete this form, gain consent from your parents /guardian and your head of learning. Then return it, with your laptop to the ICT support office.

Terms and Conditions:

All ICT use should be reasonable and appropriate for educational college purposes.

All internet access is monitored by educational ISP providers and any inappropriate or illegal use is reported to the relevant authorities.

Your laptop will be required to have configuration and maintenance procedures carried out and you will have to ensure your data is backed up and secure prior to these procedures. When requested you will make your laptop available to the technical support department to check for appropriate configuration settings.

You will be required to have current virus protection on your laptop running at all times to protect your laptop and the college network facilities.

You will have to provide details of your laptop so we can identify internet use across the college network.

All use will comply with all current legislation in terms of copyright, data protection, computer misuse and all college ICT policies.

This service is not guaranteed and may be cancelled or deactivated for technical or investigatory purposes.

When you leave the college you will take your laptop to ICT support to allow them to disable your access.

Student:

I have read and agreed the above conditions.

Student's Signature: _____

Print Name: _____

Date: _____

Parent / Carer:

I have read and discussed the above conditions with my son/daughter and I agree to the provision of this service:

Parent/Carer Signature: _____

Print Name: _____

Date: _____

Head of Learning:

I agree to this student being allowed access to the college internet on his/her personal laptop as I feel they will make appropriate use of these facilities.

Parent/Carer Signature: _____

Print Name: _____

Date: _____

Appendix H: SIMS Remote Access Form

Staff SIMS Remote Access Form



The college can provide you with SIMS Remote access via VPN technology using the Internet.

You will need to read the terms and conditions of this service and if you agree to them please complete this form.

Terms and Conditions:

All SIMS use should be reasonable and appropriate for college purposes.

You will be required to have current virus protection on your laptop/PC accessing SIMS. This will be running at all times.

All use will comply with all current legislation in terms of copyright, data protection, computer misuse and all college ICT policies.

All access will be recorded and monitored.

Your login is to be used by yourself only.

You are personally responsible for all data accessed, updated and amended with your login details.

Your remote access will be supervised at all times.

Staff:

I have read and agreed the above conditions.

Signature: _____

Print Name: _____

Date: _____

ELT Member:

This member is authorised to remotely access SIMS

Signature: _____

Print Name: _____

Date: _____

Appendix I: Social Networking Use Application Form

Social Networking Use Application Form



Please complete this form when applying for the college use of a Social Network Site.

Name of Applicant: _____ **Position** _____

Name of Site: _____

URL Address of Site: _____

Benefits of Site Use:

Intended Users of Site:

Available Security Features, Recommended Settings and Training to be provided:

Terms and Conditions:

All Social Networking Sites use should be reasonable and appropriate for college purposes.

All use will comply with all current legislation

Regular checks of appropriate use should be carried out.

Your login is to be used by yourself only.

You are personally responsible for all posts accessed, updated and amended with your login details

Any posts which are deemed inappropriate by the College must be removed immediately.

Staff:

I have read and agreed the above conditions.

Signature: _____

Print Name: _____

Date: _____

ELT Member:

This Social Network Site is authorised for College use for the above purposes.

Signature: _____

Print Name: _____

_____ Date:

Honiton Community College Academy Trust

Bring Your Own Device Policy

As the latest technological developments continue to change the world Honiton Community College will allow personal electron devices to connect to our wireless network to encourage the use of these devices for education purposes. Students, teachers and guests will be able to register their device and connect to the internet via our filters and tracking facilities.

Responsibility

Responsibility to keep the device secure rests with the owner. Honiton Academy Trust, nor its employees, are liable for any device stolen or damaged on the College Campus. If a device is stolen or damaged it will be handled through the College polices similar to other personal belongings. It is recommended that decals, other custom touches and UV marking are used to physically identify the device. Protective cases are recommended to prevent accidental damage. If the device can be tracked or disabled via carrier signal or GPS then this should be activated. All appropriate antivirus software must be installed and updated to be used on the network.

BYOD Procedures:

The College will provide three SSIDs (Network Identifiers). HCC_Staff, HCC_Students, HCC_Guests.

HCC_Staff: will allow staff to access to the internet and staff files on the servers. This is the primary wireless connection for employees and will be used for staff equipment and personal devices. Staff will present their device to ICT Support to be added to the network. A log of devices added along with their owner's details will be kept. The Staff ICT AUP must be followed at all times when using personal devices.

HCC Students: Will allow students to access the internet via our filters and logging facilities. Students and their parents will need to complete the 'Student Device Network Application Form'. The acceptance of the agreement will be logged along with device's identification details, student contact details, and any relevant User IDs. If the student application is accepted the device will be securely added to the network following ICT support protocols.

HCC_Guest: Will allow guests to the College to access the internet via our filters and logging facilities. The password for this will be changed regularly and only given to College Visitors.

BYOD Student Agreement

- I will only use my device responsibly.
- I will ask the teachers permission before using any device during lessons.
- I will only use sites allowed by the college filters.
- I will be responsible for the security of my device at all times.
- I understand I must follow the ICT AUP at all times.
- I understand that all activity is logged and may be accessed by the college.
- I understand the College has a right to confiscate and examine any device and may pass them onto other agencies.
- I understand the College will inform parents or guardians of any misuse and if the device has been confiscated it may be only returned to parent or guardians.
- I understand that this privilege may be removed in the event of inappropriate use or if the college requires additional bandwidth for educational purposes.

BYOD Network Management

All use of the wireless network will be regularly monitored. College leadership will be informed of use on a regularly bases and any essential College use will be given priority when bandwidth limits are used. Any inappropriate use will be logged and reported to a member of the College Leadership or the appropriate head of year who will decide a suitable action in line with college policy.

Honiton Community College Academy Trust

Bring Your Own Device (BYOD)



Student Device Application Form

To have your personal device added to the College Wireless network this form will need to be complete and taken with the device to be added to ICT Support. By completing this application form you agree to follow the student agreement at all times.

BYOD Student Agreement

- I will only use my device responsibly.
- I will ask the teachers permission before using any device during lessons.
- I will only use sites allowed by the college filters.
- I will be responsible for the security of my device at all times.
- I understand I must follow the ICT AUP at all times.
- I understand that all activity is logged and may be accessed by the college.
- I understand the College has a right to confiscate and examine any device and may pass them onto other agencies.
- I understand the College will inform parents or guardians of any misuse and if the device has been confiscated it may be only returned to parent or guardians.
- I understand that this privilege may be removed in the event of inappropriate use or if the college requires additional bandwidth for educational purposes.

I understand that this privilege may be removed in the event of inappropriate use or if the college requires additional bandwidth for educational purposes

Student Name _____ **Tutor Group** _____

Device Type (please tick) Mobile Phone, Tablet, Laptop, Other

Device Manufacturer _____

Device Model _____

Device Operating System _____

Student Mobile Phone Number _____

I have read the BYOD Student Agreement and accept its conditions;

Signed Student _____ Date _____

I have read the BYOD Student Agreement, accepts its conditions and give permission for my child's device to be added to the College Network.

Signed Parent _____ Date _____

Document Change History

On the 26th March 2014 the following changes were adopted by the Full Governing Body:

- Review cycle amended to 'every 2 years'.
- Additional sentence added to 'Social Networking Sites, Procedures' - These are embedded in our acceptable use policy and shared on the college website, discussed in lessons and assemblies for students and covered during training for staff.
- Additional section 'Bring your own device' added.