



CLYST VALE COMMUNITY COLLEGE

Use of ICT Policy

Reviewed: January 2017

**Date approved
by Governing Body: 10th November 2014**

Review Schedule: Annual

Next review Date: October 2017

Responsibility: Curriculum Learning & Teaching

All users will sign to accept the relevant sections of this policy annually

Company Number 07564519
A Company Limited by Guarantee
Registered in England
Clyst Vale Academy Trust, known as Clyst Vale Community College, is an exempt charity

Contents:

Student Policies:		page
	Internet Usage	3
	Network Usage	5
Staff Policies and guidelines:		
	Internet usage	7
	Network usage	9
	Laptop usage	10
	Bring Your Own Devices	11
	Guidelines for SIMs and Public Data storage	13
	ICT Facilities and Support	14

Clyst Vale Community College

STUDENT Acceptable Internet Usage Policy

The College believes that using the Internet has educational benefits to all students and staff. Internet access enables students and staff to explore thousands of libraries, databases, and bulletin boards. They will also be able to exchange messages with other learners and teachers throughout the world. However, students and families will wish to be aware that it is possible to access material which is inaccurate, defamatory, illegal, or potentially offensive to some people. To help prevent students viewing or communicating inappropriate material, Clyst Vale has taken the following steps:

- Students are taught how to use the Internet responsibly as part of their Key Stage 3 ICT course.
- Internet access in all lessons is supervised by a member of staff.
- All students have access through the open learning resources room (IT1) during certain times of the day for printing homework and supervised homework sessions. This usage is remotely monitored and logged by the system and protected by the filtering and blocking systems detailed below.
- BT provide the fibre optic dedicated leased line services into the College. The College in-house IT department manage the firewall and internet filtering in and out of the College. Clyst Vale users are given access to the internet based on age/year group. Web site access is additionally filtered on key words and URL's. This means that students are unable to type in specific Internet addresses leading to inappropriate sites, and they can also not type in certain words in search engines to find inappropriate sites. If they attempt to do this, a warning page will appear on the screen, access disallowed and logged on the filtering system.
- Chat rooms, social networking sites and non-moderated media streaming and download sites are filtered unless required by the curriculum.
- All sites visited are recorded by the internet servers and these lists are regularly checked for any inappropriate use. Any sites visited that are deemed inappropriate will be added to the filtering list and the student visiting the site warned / removed from using the internet / computer system depending on severity. Where this involves child protection issues parents and other agencies will be informed as appropriate.
- All ICT suites and laptop banks can be monitored and controlled by members of staff using the "Impero" software. This software also records inappropriate use of the internet and allows staff to block sites.
- Students are not permitted to buy or sell items through the College systems. They must not register for any additional services using the College systems, unless specifically authorized by a member of staff or required by the curriculum.
- Attempting to bypass any filters will result in a ban from all ICT

Any inappropriate use of the college's computers and Internet systems will result in the removal of the student's computer access.

We do believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. However we understand if parents do not wish their children to have access to the Internet and we will remove students' access rights if requested. If any parent does not wish their child to access the Internet at Clyst Vale we request that they write a brief letter to their Head of School who will take the appropriate steps with the technical team to remove access.

Use beyond the College Network

Students use of the Internet outside College and through handheld devices that operate outside the control of the College network are the responsibility of parents and they should refer inappropriate use to the police. However, abuse of social networking inevitably impacts on the College community and the College will seek to prevent misuse through formal and informal education and deal with bullying issues of all types robustly.

In the case of cyber bullying or other abuse of social networking being reported to College staff the College's role is to:

- Inform all parents involved and mediate restorative action
- Advise/remind parents of a bully on action to prevent a recurrence
- Advise/remind victims parents that it is their role to capture the onscreen evidence and make a complaint to the police
- Withdraw the privilege of carrying any personal device in College where a student has abused social networking

Clyst Vale Community College

STUDENT Network Usage Policy

It is our belief that students can enhance their learning by the use of computers. It is also important that students have the knowledge and skills to use computers appropriately, effectively and responsibly when they leave the College and progress onto further education or employment. To this end Clyst Vale provides access to the College network for all students. However it is important that students take responsibility when using the network facilities. Clyst Vale expects that **all users** of the network:

- Will not attempt to cause physical damage to the computer hardware, including networking equipment.
- Will report any such damage, caused or found, to the teacher in charge.
- Will not attempt to access system files, delete any files, folders or software from the network that will damage or hinder performance of the network and any associated systems.
- Will not add any files, folders or software to the network that will damage or hinder performance of the network and any associated systems.
- Will not access any games software other than that on the Approved Educational Games List.
- Will not eat or drink whilst using the College network systems.
- Will not reveal their password to anybody else and to inform the teacher or ICT Dept if their password has been compromised.
- Will not attempt to login as anyone else, nor use a machine that has been logged in for somebody else to use.
- Will not add any illegal, racist, defamatory or pornographic material to the college network, by any means. Where this involves child protection issues parents and other agencies will be informed as appropriate.
- Will not connect any computer to the college network unless specifically instructed to by a member of staff.

Students all have their own email account. Any inappropriate emails sent by users will result in an e-mail ban or removal of ICT access for a period. E-mails and attachments containing foul or abusive language are deemed as inappropriate.

The server records who has logged on to what machine and consequently damage can be traced to the person using that machine. Users are responsible for the machine they are working at and they will be charged for any parts or labour required to repair that machine, if the damage is found to be deliberate.

Users should consequently:

- Check their machine for damage before use and report any problems to the teacher in charge immediately.
- Not reveal their password to anyone else. It is not an excuse to imply someone else knows a user's password.

Inappropriate use of the college network will result in the disablement of the accounts of those involved.

Clyst Vale Community College
STAFF Acceptable Internet Usage Policy

The College believes that using the Internet has educational benefits to all students and staff. Internet access enables students and staff to explore thousands of libraries, databases, and bulletin boards. They will also be able to exchange messages with other learners and teachers throughout the world. However, everyone will wish to be aware that it is possible to access material which is inaccurate, defamatory, illegal, or potentially offensive to some people. To help prevent students viewing or communicating inappropriate material, Clyst Vale has taken the following steps:

- Internet access is filtered by our Smoothwall filters and is restricted to largely work related websites.
- Staff have a different access policy to students allowing greater freedom of the internet.
- Staff have unfiltered use of YouTube.
- All users Internet usage is monitored and logged by the system.
- BT provide the fibre optic dedicated leased line services into the College. The College in-house IT department manage the firewall and internet filtering in and out of the College. Clyst Vale staff are given access to the internet additionally filtered on key words and URL's. This means that staff are unable to type in specific Internet addresses leading to inappropriate sites, and they can also not type in certain words in search engines to find inappropriate sites. If they attempt to do this, a warning page will appear on the screen, access disallowed and logged on the filtering system.
- All sites visited are recorded by the internet servers and these lists are regularly checked for any inappropriate use.
- Chat rooms, social networking sites and non-moderated media streaming and download sites are filtered unless for curriculum use.

All ICT suites and laptop banks can be monitored and controlled by members of staff using the "Impero" software. This software also records inappropriate use of the internet and allows staff to block sites.

Staff are discouraged from buying or selling items through the College email system although it is not prohibited

Some Answers to Frequently Asked E-Safety Questions

Can I use my school email account to register for non-work related web sites and services?

No, registering for non-work related subscriptions and web services increase the spam received by the College. Gmail, Hotmail accounts are free

Can I use a school computer to book holidays etc during lunch time or after school?

Yes, our current usage policy does not prohibit personal use in your time but such use would be unprofessional during working hours.

Can I respond to a comment about the school on Facebook?

No, do not respond to any post on Facebook directly, refer your concern to your line manager or SLT.

How should I respond if I am subjected to cyber bullying by pupils?

Do not respond directly online, refer your concern to your line manager or SLT

Can I use my mobile to take photos or videos on school trips?

This should be avoided, mobile phones are not secure and you should not hold pictures of students on an insecure device. Use a camera, ideally a college camera.

If you have to use a phone images should be transferred to the College system at the earliest opportunity and deleted from the device. If images are emailed this should only be done using a College email account.

Should I text a pupil in the evening to remind and encourage him to complete a project?

No, under no circumstances use text messaging with pupils. It is not open and transparent and so is potentially suspicious. Use school email or a Moodle forum and include the whole group in any invitation to use email.

Should I continue to use my social network site?

Yes but apply all the privacy settings (see the guide) and under no circumstances accept students or the 'Friends' of students as 'Friends'.

Can I use social media to discuss a topic with my students?

No, use a Moodle forum.

Can school limit my private online publishing?

You should never publish (put on the web) anything that is not work related using College resources and devices (including your laptop).

In any case be very careful to only publish items that clearly meet the GTC professional standards on any site that is open to the WWW.

E.g. don't put embarrassing pictures on an unprotected Facebook page!

Remember all the guidance and the GTC policy are in Moodle (Staff CPD/iTeach).

Clyst Vale Community College

STAFF Network Usage Policy

It is our belief that staff can enhance the learning by students through the use of computers. It is also important that staff have the knowledge and skills to use computers appropriately, effectively and responsibly. To this end Clyst Vale provides access to the College network for all staff. However it is just as important that staff take responsibility when using the network facilities. Clyst Vale expects that **all users** of the network:

- Will not attempt to cause physical damage to the computer hardware, including networking equipment.
- Will report/investigate any such damage, caused or found.
- Will not attempt to access system files, delete any files, folders or software from the network that will damage or hinder performance of the network and any associated systems unless instructed by the ICT dept.
- Will not add any files, folders or software to the network that will knowingly damage or hinder performance of the network and any associated systems.
- Will not reveal their password to anybody else and to inform the ICT dept if their password has been compromised.
- Will not attempt to login as anyone else, nor use a machine that has been logged in for somebody else to use.
- Will not add any illegal, racist, defamatory or pornographic material to the college network, by any means.
- Will not connect any computer to the college network unless approved by the ICT dept.
- Students should never use staff logins to work on a computer. Access to staff emails and full Admin drive will be available to that user!

The server records who has logged on to what machine and activities monitored.

STAFF Laptop usage policy

Many staff will have the loan of a laptop whilst employed at this college and hence while the laptop is in your care the following items should be noted:

By using the laptop provided, staff must agree to the following conditions:

- The laptop remains the property of Clyst Vale Community College and is only for the use of the member of staff it is issued to.
- As the laptop is the property of Clyst Vale Community College it will be replaced by the college if stolen or lost, provided you can demonstrate that you took reasonable care and attention.
- Only software licensed by the College and installed by the college's ICT staff should be used.
- File Sharing, torrent software and Peer to Peer networking software is strictly forbidden.
- Should any faults occur the college's ICT staff must be advised as soon as possible so that they may undertake any necessary repairs. Under no circumstances should staff attempt to fix suspected hardware faults. These are carried out only by the college's ICT staff.
- Training in the use of the laptop and how to access the Curriculum Network, Internet and email can be provided by the ICT staff if required.
- Any telephone charges incurred by staff accessing the internet from home or on their own devices are not chargeable to the College.
- Devon and College policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to by all users of the laptop.
- Staff are required to read all documentation provided with the laptop and follow the recommended procedures
- Data that is held on the laptop is the users responsibility. User is responsible for backing up any required data.
- AntiVirus configurations should be set by the ICT dept
- Windows Updates – When Update icon appears on the System tray, updates must be installed when convenient but asap.
- Students should not have access to your laptop under any circumstances. The full F drive/ Admin drive will be accessible by that student under your login.
- You must report any fault (this may be cosmetic) to the ICT Dept as repairs maybe done under warranty.

Clyst Vale Community College

BYOD (Bring Your Own Device) policy

Who owns the stored data?

On a smartphone, a student or staff member may have several work and personal email accounts accessible from their phone but any Clyst Vale email data stored on a smartphone is the property of Clyst Vale and will fall under College security protocols as some of the data could be commercially sensitive and highly confidential.

Monitoring of emails

Clyst Vale monitors all emails in and out of the College using MailMarshal per our ICT policies, but will not, and cannot, monitor any non-clyst Vale email accounts accessed via a smartphone.

Smartphone use on College network

This will be granted on a case by case basis and will only be granted if smartphone is used for teaching purposes. There will need to be adequate antivirus protection if deemed necessary by the College.

Loss or theft of smartphone

The loss or theft of a smartphone is a relatively common problem, and Clyst Vale reserve the right to delete College data stored on a personal smartphone. If a smartphone has been lost or stolen, the user should report it to the ICT department so action can be taken.

Every student or staff member that connects to the College Exchange server using activesync can “remotely wipe” their smart phone in this case. The ICT dept. can also action this.

Agreeing to this policy

By configuring your smartphone to receive and send College emails from your smartphone means you agree to the College’s terms and conditions of use and Clyst Vale cannot be held responsible for any loss of data relating to your smartphone.

Security Restrictions

When you configure your phone to connect to the College email server, the following restrictions will apply:

- 4 digit PIN-based access; this will be enforced on the handset, not just the email account. This can be removed only if you remove the email account first.
- PIN-based lockout; (eg the smartphone will be locked after 8 PIN code attempts. It will be locked for 1 minute after 8 attempts.
- Remote Wipe function: You and the ICT dept can remotely wipe your phone if lost or stolen. This will be a last resort action and Clyst Vale will not be responsible for ANY data lost on the users handset. This is a good feature for you as it means that you have the control

Like any system, it is recommended that you backup your smartphone/device if important data could be lost

Protecting our network/systems

Students and Staff may not install apps to gain access to the school network for non-work purposes. Any attempts to compromise the school systems will mean your device will be removed from accessing our systems and probably wiped prior to removal.

The ICT Terms and Condition of Use still apply to devices connecting to our systems

Use of Smartphones and other personal devices for photography and audio recording

While the College encourages the use of photography for educational purposes and publicising College events through the web site, staff need to be mindful of child protection protocols at all times. If a personal Smartphone is used to photograph a College event:

- images should be transferred to the College system at the earliest opportunity and deleted from the device.
- if images are emailed this should only be done using a College email account.

This also applies to any video or audio recordings made with a personal device.

A Smartphone or other audio recorder should not be use by any member of staff to record any meeting without seeking the permission of all those present at the meeting.

Clyst Vale Community College

STAFF Guidelines for users of SIMS and the Public data store

The SIMS system is in constant use by the admin/finance office. It is a vital part of running Clyst Vale. You may have access to SIMS. Please take care. To register for access to the SIMS system, please contact the SIMS administrator; Linda Smith

Security

- Offices should be kept locked.
- Do not leave SIMS open. A password-protected screen saver is a useful level of security and should be used.
- Ensure you log out of your laptop/PC every day (not hibernated)

Passwords

- These are for individuals and not for groups.
- **Do not share your user ID or password.**
- Do not leave notes lying around with this information on. You need to remember your user ID and password. It is needed to access SIMS. Please contact SIMS administrator, if you have any difficulties.

Software on Admin computers

Any additional software installed should be from a legitimate source and you should have a licence (if appropriate). Do not install additional software onto Admin computers unless sanctioned by the ICT Dept. Please do not download screensavers from other sources.

Data Protection

We are registered with the Data Protection Agency. The data we hold is confidential and must not be passed on. An individual parent/pupil is entitled to see the data we hold on them but this is best done by printing it out and handing it to them. Pupils/parents should not have general access (even visual) to a screen with data showing.

Virus Protection

We are registered to use the Sophos anti-virus product and this regularly updated automatically. Our registration also allows employed staff to use Sophos on their home computers. Please see the help.clystvale.org knowledgebase for details

SIMS Upgrades

Upgrades take place outside of school hours as SIMS has been moved outside the school and is hosted by SComis. Mrs L Smith is the first contact for SIMS related issues.

Clyst Vale Community College

ICT Facilities and Support Policy

The College network offers Broadband Internet access, internal/external e-mail facilities, external/Internal access to Central Resources, colour printing and scanning facilities for all staff users within the College.

The network offers each member of staff their own personal storage area to save their work in, which is only accessible by that particular staff member. A “Work Postbox” is also available to each member of staff, which enables students to copy any work to the teacher electronically for marking etc.

The colleges VLE is now provided through the Moodle platform, it is progressively replacing the “Work Postbox” and “Central Resources” in providing online resources and the setting and submission of homework.

The ICT Technicians provide support for the network which includes loading curriculum–based software, upgrading hardware, repairs to hardware, printing problems, login issues, maintenance and care of the ICT suites, SIMS connection issues, internet, e-mail, support and assistance during lessons if required and general ICT queries.

Support is provided via a Helpdesk system which requests and issue can be raised via email to the helpdesk.

For access and queries within SIMS, please contact the SIMs administrator Linda Smith