



SETTLE COLLEGE

“Learning for Success” - ICT Acceptable Use Policy



If you have any questions about the policy, please contact the ICT Network Manager or Faculty Leader of Technology.

The College assumes the honesty and integrity of its ICT users. Facilities are provided in as unrestricted manner as possible to offer the best possible quality of service.

It is the users' responsibility to ensure that they comply with the policy. The latest version can be found on the College website and in each major computer area.

All staff and students will need to sign an agreement to confirm they will abide by the policy before they are granted access to the ICT systems.

Refusal to follow any of this policy when pointed out by a member of staff will be treated as any other refusal to follow an instruction, in line with the College normal disciplinary procedures.

General Policy

The user agrees not to:

Upload, download, post, email or otherwise transmit or store any content that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful or racially, ethnically or otherwise objectionable.

Impersonate any person or entity, or falsely state or misrepresent affiliation with a person or entity including the forging headers or to otherwise manipulate identifiers in order to disguise the origin of any content transmitted through the College services.

Upload, download, post, email or otherwise transmit or store any content that the user does not have the right to transmit.

Upload, download, post, email or otherwise transmit or store any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party.

Upload, download, post, email or otherwise transmit or store any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes" etc. except when directly resulting from curriculum work.

Upload, download, post, email or otherwise transmit or store any material that contains software viruses or any other computer code, files or programs designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware; or telecommunications equipment.

Interfere with or disrupt the service or servers or networks connected to the service, or disobey any requirements, procedures, policies or regulations of networks connected to the service.

Collect or store personal information about others without direct reference to The Data Protection Act.

To use the College's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes unless as part of a curriculum project.

Revised:080709

Visit or use any online messaging service, "chat site", web-based email, discussion forum, online-gaming / social networking sites not supplied or authorised by the College.

Store or use any software not specifically installed on the service by an authorised person.

Visit, use, download, or store any game, either application or browser-based, without permission of a member of the ICT Team. Users should also not bring any games into College on external storage mediums such as Pen Drives, Portable Hard Drives and other similar devices, if they are found to do so they may be subject to having the device removed and the usual College disciplinary procedures invoked.

The College reserves the right to refer any breach of this policy to the respective Form Tutor / Head of House and / or member of the Senior Leadership Team. This may result in the suspension of any or all parts of the services provided.

Network Services

This comprises of access to workstations (PC or Mac) in the various classrooms, and other areas for all users, and for staff additional access in departmental offices, work rooms and staff areas.

Storage of files for all users is available on the main file Server, which is backed up daily during term time (Mon – Fri), and up to three weeks worth of backups are normally held.

Each user is allocated a Quota for File Storage; if this is reached the user will be unable to save new files. If this occurs they should see the ICT Support Team who can look into increasing the quota if all files are stored related to College matters and sufficient space is available on the College File Servers. Users should not use the College File Servers for storing non-College related materials.

All users shall have access to any files they have created, except where ownership / authorship are in question. This is then referred to a member of the Senior Leadership Team.

Each user shall have a unique login ID and password. The password must not be divulged to any other user or any third parties outside of the college. If you believe that this has been breached you must contact the ICT Support Team and inform them immediately and they can reset the passwords for any ICT Service that the College provides to ensure the security of the College Systems.

All passwords must be changed ever month (30 days), this is prompted by the system automatically in some cases, if the system doesn't prompt, the user should change them manually. Users should not write down password, or choose ones that are easy to guess or common such as "password". They should contain a minimum of 6 characters and contain a number. Users are suggested to think of replacing letters with numbers to assist in making a simple password more complex, such as using "1" in place of an "l".

Internet Services

Each User shall have an Internet account to access the Internet via the College's Proxy Server. The Proxy Server will filter any unwarranted materials and be updated regularly to maintain this high level of filtering.

Any user repeatedly attempting to access such material will have their account automatically locked and it will not be reopened until they have discussed the matter with a member of the College ICT Staff, Faculty Leader of Technology, Head of House or Head of Sixth Form .

The College does not pre-screen content viewed by users, but relies on the filtering software. Should any site or content be discovered which does not comply to the General Policy it will be added immediately. We ask users to assist us with this by informing us of any offending material to allow it to be added to the "block list" of sites.

E-Mail Services

Each user shall have an E-mail account hosed on the Local Authority Provided Email system to enable them to send mail internally and externally.

The size of each user's mailbox (mail storage area) will be decided by group and/or requirements to do work. Staff will receive a greater sized mailbox than students. The limits for these are set by the Local Authority and, at present cannot be changed.

Mail sent and received shall be filtered for language, content and certain file types within attachments. If a user sends an email that is caught by the filters, the user will be notified by an automated email from the Email System and they should look into the cause of the block and resolve it as required, this includes forwarding the email on to the address specified in the E-mail to allow a blocked e-mail to be released. If help is required please contact the ICT Support team.

Any user who receives unsolicited mail can inform the ICT Network Manager who will endeavour to work with the Local Authority to trace the originator and report them to their Service Provider, clearly asking for the originator's account to be terminated if the mail has been in breach of the Service Provider's Terms of Service.

Likewise, if any user is found to be sending unsolicited emails, to other users within the school, or to external accounts, the matter will be referred to the College ICT Staff, Faculty Leader of Technology, Head of House or Head of Sixth Form who will take appropriate action based on College discipline procedures.

Virtual Learning Environment

Each user shall have an ID and password on both College maintained Virtual Learning Environments (VLE). These are both hosted externally, one by the arrangement of the ICT Network Manager (Moodle) and the other by the Local Authority (Fronter). The College is transitioning over from Moodle to Fronter over the next 2 years.

Users will have storage space for an E-Portfolio on the Fronter VLE, this space is governed by the Local Authority as well as by the College's storage allocation on the system. If you fill this allocation please contact ICT Support to look at an increase.

All users will be given instruction on how to use the VLE platforms in College and will find a wealth of useful information in relation to the College subjects and this will enable Student to have access to the curriculum and resources for Home Study and Revision Purposes.

If a user's unique login ID or password is forgotten or has

potentially been divulged to any other user or any third parties outside of the college, you must contact the ICT Support team and inform them immediately and they will reset your password for you.

Security

Each User will be given a unique ID and password that will allow them to access their computer account. The same password will allow them to access their "Home Area" on one of the College File Servers, the ICT Helpdesk and their Internet account. They will have a separate ID and password for their Email account, Virtual Learning Environment (VLE) and access to the College's Management Information Systems (Serco). If an ID or password is forgotten, they can be changed / retrieved by a member of the ICT Support Team.

The ID and password are solely the responsibility of the user and not to be shared with other users or third parties for any reason. If a user is found using the ID and password of another user their access may be suspended and immediately referred to their respective Form Tutor / Head of House, Head of Sixth Form or ICT Network Manager who will take appropriate action based on College discipline procedures..

The only programs that may be used within the College are those agreed on by the ICT Network Manager and/or Leadership Team of the College and installed by a member of the ICT support team. The introductions of programs (including any software containing viruses or used to disrupt any part of the Network, security software or connected networks) onto the network is not tolerated and will be treated as intentional damage or an attempt to cause damage to College property.

All information about staff and students will be dealt with in compliance the Data Protection Act and only given to authorised agencies. Staff and students agree to abide by the Data Protection Policy.

The College reserves the right to monitor all traffic on the network, either manually or through automated software, to ensure policy compliance and to aid in resolving any issues.

Treatment of Equipment

The ICT support team will endeavour to ensure all equipment is in working order. They will set targets for the quality of service they provide, which will be monitored regularly by the Faculty Leader for Technology.

Should any user find that a piece of equipment does not work correctly they are to report it to a member of the ICT support team and not attempt to repair it themselves. This can be via the ICT Helpdesk for non-critical repairs, or via Telephone or Email to the ICT Support Team. "Corridor" requests are not acceptable as these can be lost and forgotten.

Any user who causes damage intentionally or through neglect to any equipment may be refused the right to further use of the equipment and may be asked to cover costs towards any repairs or replacements.

Unless otherwise issue to a member of staff as part of their contract (e.g. staff laptops) any equipment taken off site is the responsibility of the user and you are advised to check that its loss or damage is covered by your personal insurance. All such loans will require a signature by a parent / teacher and the ICT Support Team.

Creator: STJS / STGRS

Document Ref: AUP001