Robertsbridge Community College - Computer / Network Acceptable Use Policy (AUP)

Disclaimer

The computer systems are owned by the College, and are made available to staff, students, governors and the community customers to support and enhance education. Robertsbridge Community College will endeavour, wherever possible to provide a safe and secure environment for its users. However please be aware that it cannot guarantee complete safety from inappropriate material. The responsibility must lie with each individual to use ICT in a safe, sensible and responsible way.
This AUP has been drawn up to protect all parties. Anyone who fails to comply, or acts in a way which may be deemed inappropriate, or irresponsibly may lose access rights to College computers. I n the case of students, parents/carers may be informed. In exceptional circumstances, where there are reasonable grounds to suspect a user has committed a criminal offence the police will be informed and a criminal prosecution may follow.
Anyone who uses a College computer network, computer, tablet or device must read the enclosed AUP carefully. Please sign this copy, and keep a copy for your records.

- I will only use the College network, and associated access devices, intranet and VLE with the username, and password which I have been given. I agree not to share this information.
- I will not allow the use of my computer account to be used by any other person other than the IT technical support team.
- I will not access other peoples files unless through shared work areas (Except when authorised by the Headteacher)
- Any use of computers will not involve activities that could be damaging to the College, and its reputation.
- I will only send or receive materials or data which is polite, and responsible. It must not violate any law, or regulation, be defamatory, offensive, abusive, indecent, obscene, or constitute harassment.
- Students will only use email with staff approval, and will not give out personal information on line.
- I will report immediately any unpleasant material or messages sent to me or accessed by me.
- I understand my report would be confidential, and would help protect everyone.
- I understand that the College may monitor my computer use, check any data held on the College network, and may monitor the internet sites that I visit.
- I understand that the College reserves the right to delete any files held on its computer systems or network.
- I will not download, or install anything that may threaten the school ICT systems
- If Issued with a laptop computer, tablet or device, I agree to bring it into school as requested.
- No software should be installed without the consent of the Network manager, who will ensure compatibility, appropriateness and licensing requirements are met.
- I will not use the school computer equipment to play violent or age in-appropriate games. I will respect the legal protection provided by copyright and licence to programs, data, images and music stored on the network.
- I will not plagiarise works that I find on the internet, or other sources. (Plagiarise is tasking the ideas or writings of others and presenting them as if they were yours)
- I agree not to use the Robertsbridge network and associated devices for personal use, or to run any business outside of the College.
- I have read and accept the full College acceptable use policy

I agree to abide by the rules of the computer acceptable use policy

Staff / Student Signature _____

Print Name _____

Date ___/___/___

If Applicable:- Mentor Group _____ Parent / Carer Signature _____

ROBERTSBRIDGE
COMMUNITY COLLEGE

Robertsbridge Community College Computer Network Acceptable Use Policy (AUP)

This policy applies to employees, temps, freelancers, volunteers and contractors working at Robertsbridge Community College.

This policy describes acceptable (and unacceptable) use of the College's Networks and must be read and followed by all Authorised Users.

Information Processing Equipment, Internet, Intranet and e-mail access provided by Robertsbridge Community College is intended for College use only, but limited access for personal use is allowed at lunchtimes and at the end of the College day. The College encourages the use of the Internet and e-mail, because they make communication and research more efficient and effective.

Use of the Colleges time, facilities, equipment or supplies for an employee's or contractors' private business is prohibited. This AUP has been created to ensure that all employees, volunteers and contractors understand the basis on which access is allowed

This AUP includes references to information security, 'netiquette' use and misuse of the Robertsbridge Community College Electronic Networks and Information Processing Equipment.

Where there is a requirement to attach to College Electronic Network with high levels of access, from insecure locations (Public areas, cyber cafes etc.) Authorised Users will be requested to sign acceptance of this policy and send the summary sheet to the Network Manager (Richard Leaney)

AUP Index

Definitions

Authorised User

- An Authorised User is a College employee, volunteer, contractor or a temporary College staff member, a member of East Sussex County Council service provider's staff, a freelancer, a contractor or other person not directly employed by the College who has been authorised by or on behalf of Robertsbridge Community College.

Computers

- An electronic device that processes data according to a set of instructions. Computers include but are not necessary limited to the following:
  Desktops, towers, laptop, netbooks, mobile phones, kindles, Kobo or tablet devices.

Data

- Information that is stored electronically on a computer, SAN, Server or other storage medium.
- Sensitive data is data that requires a high level of protection because its unauthorised disclosure could harm students, staff or bring the College into disrepute.

Download

- Downloading is the act of transferring data from remote Information Processing Equipment to local Information Processing Equipment and optionally storing it on local Information Processing Equipment.

Electronic Network

- An electronic network is a group of Information Processing Equipment that can communicate with/via each other. Electronic Networks include but are not necessary limited to the following:
  - The public Internet;
  - Networks internal to Robertsbridge Community College
  - Contracted service provider networks; and
  - public and private networks external to the College

Information Processing Equipment (IPE)

- Information processing equipment includes, but is not necessarily limited to, a personal computer, laptop, wireless communication device, personal digital assistant, hub, server, SAN, communications equipment, or console device that may be connected, once authorised, to the Colleges Electronic Network.

College Intranet/Shared Access

- An intranet is a private network that is contained within the college. It may consist of many interlinked local area networks and also use leased lines in the wide area network. The main purpose of an intranet is to share College information and computing resources among employees. An intranet at the College has become known as the Public / Library drive and the SharePoint Server.

Internet

- The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks.

School Information Management Systems (SIMS)

- Sims is the main database that holds all staff and student data, this includes all personal details, timetables, Assessment and sensitive information.

Overview

Compliance

- It is the responsibility of each Authorised User to take all reasonable steps to ensure compliance with the conditions set out in this AUP document, and to ensure that Prohibited Use of College Information Processing Equipment does not occur. It is preferable for misuse to be prevented by a combination of technical solutions and responsible attitudes to the use of College Information Processing Equipment on the part of users. Where violation of these conditions is illegal or unlawful, or results in loss, alteration or disclosure of Data or the College Information Processing Equipment, the matter may be referred the head for further action.
- This also assumes that all Authorised Users have read and comply with the College E-Safety Policy as laid down by the E-Safety committee. (Doug Hanson, David Evans, Darren Eglington and Paul Foxley)

Expectation of Privacy

- Users should assume that electronic communications across the Internet cannot be considered private or secure and should consider the sending of confidential, sensitive or personal information (sensitive and personal information are as defined by the Data Protection Act 1998) by other means. College Information Processing Equipment are subject to tracking (using logging and audit facilities) for purposes of ensuring compliance with College policies, system administration, maintenance and security as part of the normal course of College business practice. Monitoring is permitted for the purposes of a specific investigation and detailed under the College policy on the Regulation of Investigatory Powers Act 2000. The Data Protection Act 1998 also contains monitoring clauses.

Statement of Use

- This AUP provides direction to Authorised Users on the use of College Information Processing Equipment. Uses of College Information Processing Equipment are separated into the following categories.
    - Authorised Use;
    - Personal Use;
    - Prohibited Use.

  Authorised Users shall only use the College Information Processing Equipment for Authorised Use and Personal Use. Authorised Users shall not use College Information Processing Equipment for any Prohibited Use.

Condition for use

Authorised use

- Authorised use is the use of College Information Processing Equipment to carry out the duties as per your contract of employment or permission granted by the systems manager or SLT member to use College Information Processing Equipment to carry out duties that assists in allowing the College to function effectively.
- Communicating with colleagues using email, use of SIMS, use of all College licensed software and use of the internet for you to carry out your contracted duties. Circumventing these systems would be considered Unauthorised Use.

Personal Use

- Personal use is the use of Robertsbridge Community College Information Processing Equipment which does not fall in line with your day to day contracted duties.
- Use of personal mobile devices during contracted time at the College
- Use of the electronic software to communicate with friends and family, online banking, shopping of personal and family items.
- Use of College Information Processing Equipment may only be used for a reasonable duration and frequency and shall not interfere with the performance of the contracted duties and functions of an authorised user or any other person.
- Personal use may be authorised by the Authorised user's line manager.
- Personal use of the internet is not considered part of an authorised user's contracted time at the College.
- SLT, Line Managers and Systems Manager may restrict personal use of College Information Processing Systems if the integrity of the College comes under threat or disrepute.

Prohibited Use

- Prohibited use is the use of College Information Processing equipment that is not:
    - Authorised Use.
    - Personal Use.
- Prohibited uses of Robertsbridge Community College Information Processing Equipment include, but is not necessary limited to:
    - Personal use that exceeds a reasonable duration.
    - Personal use that interferes with performance or official duties of an Authorised User or other person.
    - Any use that results in personal financial gain, e.g. electronic gaming (exception to this is any financial gain acquired through legitimate competitions/Games held at the College)
    - Peer to peer networking/content sharing software to transmit any College data in or out of the College/East Sussex County Council
    - Accessing or distributing any material that contains pornographic, sexual acts, nudity and incitement of hatred.
    - Downloading or use of illegal or unauthorised programs. College Information Processing Equipment must not modified in its software setup or should any additional programs be installed unless authorised by I.T Support technicians.
    - Usage of illegal or unlicensed software is strictly prohibited and can lead to the College being prosecuted. Software that is installed by any user can cause conflict with existing software and introduce Malware or Viruses.
    - Personal use that has been prohibited by a line manager, systems manager or SLT member.
    - Any use that would bring the College into disrepute.
    - Any use that does not comply with Copyright Law.
    - Any use that could cause harm or discredit others.
    - Any unlawful activity.
- The College maintains an Internet filtering system; it is prohibited to try to bypass the filtering system to gain access to website that may have been filtered. Staff can submit a helpdesk request to have certain sites allowed through the filtering system at which point the systems manager will make a judgement as to whether or not to allow these sites through the filtering system. Staff can take this to a higher level if they feel there has been an unreasonable decision made.

Examples

College Email

- Authorised Users must consider and conform to the following for email activities: Email communication must reflect professional and respectful correspondence standards and must not be libellous or use abusive language. Each Authorised User is responsible for the content of all text, audio or images that they place on or send over the Internet, Intranet or e-mail. No email or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else. All messages communicated on the Internet, Intranet or email system should contain the Authorised User's name. Digital communications with students must be done on a professional level using College systems only.

Copyright

- Users must honour copyright laws regarding protected commercial software, music or any intellectual property. Duplicating, transmitting, or using software not in compliance with software license agreements is considered copyright infringement. Authorised Users shall not make copies of software, music or literature in violation of copyright laws without the full legal right to do so. Unauthorised use of copyrighted materials or another person's original writings is considered copyright infringement. Copyrighted materials belonging to others may not be transmitted by Authorised Users on the Internet without permission. Users may download copyright material from the Internet, but its use must be strictly within the agreement as posted by the author or current copyright law. Copyrighted agency information used on web sites must be clearly labelled as such.

Network Security

- When connecting to College Information Processing Equipment, Authorised Users must consider and conform with the following:
    - Authentication - Authorised Users are responsible for controlling the access to their Information Processing Equipment, properly logging on and off Electronic Networks, and not using another user's Username and password. Unauthorised distribution of passwords and/or access codes is strictly prohibited, Your Username and password belongs to you, and you are responsible for all actions taken with it. Attempting to circumvent user authentication or security of any Information Processing Equipment, Electronic Network, or account is strictly prohibited. This includes, but is not limited to, accessing data not intended for the user, logging into a server or account the user is not expressly authorised to access, or probing the security of College servers and networks.
    - Any data stored on storage media (USB memory sticks, USB hard drives, CD's, DVD's or any other electronic media) that contains staff or student details must be encrypted if it is taken off the College premises. Please see the College technicians for further details on how to achieve this.
    - That you agree that all systems are monitored regularly
    - That when you leave your Computer for any length of time that you will either log off or lock the computer you are logged into.
    - That you will report any security issues to the systems manager or SLT for further investigation.

Remote Access – Home Use

- When connecting to the College network from outside the College premises on equipment that is not owned by the College, you agree that the following has been met.
    - That all devices have been updated with the latest security fixes from operating systems vendors website.
    - That Anti-virus software is installed and kept up to date with the Anti-Virus vendor's website on a daily basis.
    - That Anti-Virus/Malware scans take place on a regular basis.
    - That you are running a firewall on your local device or router to protect your own equipment from potential attack or monitoring.
    - That other family members, friends or third parties are not allowed access to the equipment whilst logged into the College network.
    - That the equipment will not be left unattended for any duration of time when connected to the College network.
    - That you will not attempt to connect to the College network if any of the above are not met.
    - That you will report any issues that you feel are suspicious by nature or seek advice from the I.T Support at Robertsbridge Community College for further advice.

Remote Access - College Equipment

- When using College Information Processing Equipment of which is under the control of the Authorised User, connects to the College Networks the following must be followed.
    - The Authorised User should be aware of the environment they are in and that the Information Processing Equipment being used is not being overlooked or in a position for third parties to read sensitive information from the screen they are working on.
    - That the College Information Processing Equipment is kept up to date with Updates from the operating systems vendors' website and that the equipment is connected to the College Network every five weeks to obtain any additional updates that the College deem necessary for the security of that device.
    - That no other Anti-Virus software is installed on the College Information Processing Equipment other than the licensed software owned by the College.
    - That no additional Software is installed on to the College Information Processing Equipment other than the software that was installed when the Authorised User took ownership of the device. (Exceptions are 2x Client which prompts to connect to the College Network on first use)
    - That the Software that is installed on the College Information Processing Equipment is not modified or reversed engineered in any way or form.
- That No personal music is stored on the College Information Processing equipment other than that of which is licensed to Robertsbridge Community College.
- The Authorised User may not modify/remove any components on the College Information Processing Equipment.
- The Authorised User takes responsibility and care of the Information Processing Equipment (**IPE**) and that IPE are <u>NOT</u> left unattended unless they are properly secured, unless it is in the Authorised Users house or locked in a safe when used on holiday.
- It is the responsibility of the Authorised User to report the loss, damage or other problems with the IPE to the College as soon a possible.

- That Unauthorised Users cannot access the IPE whilst it is in the possession of the Authorised User and that when the IPE is connected to the College Electronic Network they are not left unattended for any duration of time.

Remote Access – Public Areas (Cyber Cafes etc.)

- When connecting to the College Electronic Network using Information Processing Equipment that does not belong to Robertsbridge Community College or the Authorised User the following must be followed.
    - When accessing the College email server, Sharepoint Server, VLE or remote access server the Authorised User must delete any copies of files or webpages and must make sure these are not left on the Information Processing Equipment.
    - Printing of any College Information must not be left on any Information Processing Equipment and all files must be deleted where ever possible.
    - When viewing any emails or sensitive information in a public place, you must ensure that people are not snooping or trying to read any of the information you are accessing at that time.

Unacceptable Use

- College Information Processing Equipment may not be used for any of the following:
    - The transmission or creation of any obscene, offensive or indecent images, data or other material or any data that can be resolved into obscene or indecent images or material.
    - The creation or transmission of any data which is designed to cause inconvenience, anxiety, provocation or defamation of character.
    - The transmission of data that is copyrighted unless express permission is granted from the owner.
    - Corrupting other user's data inside or outside the College premises.
    - Disrupting the work of others.
    - Implementing Malware, Viruses, or other malicious software.
    - Using Software that is not properly licensed and contravenes the copyright of the known software.
    - Using software that has been requested not to be used by the I.T team
    - Transmission or access of any inappropriate content or graphical material.
    - Running businesses for profit or non-profitable activities.
    - Gambling.
    - Criminal activity.
    - The removal of the College Anti-Virus software unless specifically requested by I.T staff.
    - Circumventing any Proxy servers to gain access to inappropriate websites.
    - Accessing other user's mailboxes unless a written instruction is obtained from SLT or the named person's line manager.
    - Removal of sensitive data unless the Information Processing Equipment is encrypted. (see definitions)
    - Any purpose which is deemed illegal or against College policy.
    - Excessive personal use.
    - Any College Information Processing Equipment that is used to gain access to another network whereby it contravenes those networks AUP will be deemed an unacceptable use.
    - Publishing of digital Images of students without first checking the Sims database to see if consent has been given by the parents. See E-Safety Policy for further details

Failure to comply with College AUP

- The College reserves the right to take the following action if the College discovers that the AUP has been breached in any way as laid out in this document.
    - Report any findings to the named person's line manager, SLT or Head.
    - Report any findings of a serious nature to the relevant authorities.
    - Revoke any access to College Information Processing Equipment.
    - Suspend the Authorised Users account pending further investigation.

References

- E-Safety Policy located on the College website http://www.robertsbridge.org.uk/policies.htm
- Copyright http://www.ipo.gov.uk

Revised September 2015