RENDCOMB COLLEGE

NURSERY • JUNIOR • SENIOR

# Acceptable Use Policy

# PUPILS

**Monitoring:**

Deputy Head (Pastoral) and Director of ICT

**Policy Review:**

Reviewed: August 2019

Next review: August 2020

**Acceptable Use Agreement**

I understand that I must read and abide by the Acceptable Use Policy, to both keep myself safe and protect others from potential harm when using computers at Rendcomb College.

There is significant detail in the policy, that I agree to read and abide by. It's summarised by following principles:

1. I will only use the network and the College's computers for appropriate school work and communication.

2. I will act maturely and politely in all that I say and do online.

3. I will do all that I can to ensure the College's network and computers stay secure.

4. I accept that all of my actions have consequences, particularly online and so will think before I speak and treat others like I want to be treated. Anything that happens using my account is my responsibility.

5. There are many laws, both British and International, and I must comply with them. This includes the promotion of British Values and Standards and prevention of extremism.

6. I understand that the school may monitor my use of the school's systems, devices and digital communications for my own personal safety.

7. I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

8. If I, or someone I know is in trouble online, I will speak to an appropriate member of staff so that their safety can be ensured.

9. I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

10. I understand that if I fail to comply with this AUP, I will be subject to disciplinary action. This may include confiscation of personal devices, loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**I have read, understood and agree to comply with the Acceptable Use Policy.**

Name:

Date: 21/10/2019 Signed:

## Acceptable Use Policy

The Rendcomb College Acceptable Use Policy is an extension of School Rules specifically covering the use of the Rendcomb Network and any electronic equipment connected to it. The use of the Rendcomb College Computer Network and Internet via that network is a privilege and not a right, granted by the College to you the network user and should not be abused in any way. Any misappropriation of the network, or violation of the following rules and conditions is an infringement of school rules, and will therefore be met with disciplinary action.

The purpose of the Rendcomb Network is to assist the user in an academic environment as an academic tool. The intent of this policy is to set out rules for the user, to guide them in the correct usage of the network, preventing the user from misuse.

Connection to the Rendcomb Network will result in automatic acceptance of the policy and agreement to comply.

## Use and Procedures

All authorised users of the network are assigned a Rendcomb College network username and password. No person should attempt to gain access to the network using credentials that have not been assigned to them or access other users' data.

Under no circumstances should a user attempt to traverse and or bypass the Rendcomb College internet filtering system. Any security gaps identified should be referred to the IT department immediately. Failure to do so, or attempting to exploit any vulnerabilities found will be considered a serious disciplinary issue.

## Bring Your Own Device (BYOD)

The College permits pupils to use their portable devices in learning spaces as long as the class teacher has given explicit permission to do so. Acceptable devices are laptops or tablet PCs ideally with a physical keyboard. Mobile phones and on-screen keyboard only devices are not acceptable unless explicit permission is given, e.g. using cameras on phones.

When using a personal device, you must not take pictures or record videos of staff or other pupils without their permission. If these are taken for educational reasons then these images should then be transferred to the school network as soon as possible and then deleted from the personal device. If someone else asks you to delete an image or video of them stored on your device, you should do so immediately.

Your personal computer, laptop or mobile devices should:

- Have a fully licensed copy of an up to date operating system.
- Have fully licensed and up to date Anti-Virus software installed.
- Only have legal and licensed software and Apps installed.
- Users should be mindful of the age limits for App purchases and use, and should ensure they read the terms and conditions before use.
- Not store any personal data relating to Rendcomb College pupils or staff on them.

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access.
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security.
- The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

**Security**

All Authorised Rendcomb College Network users are issued with login credentials. Protecting your personal credentials is essential to the security of the network, your personal computer and your personal data. As guidance the following security rules should be followed:

- Your Password should be
  - at least 7 characters.
  - a capital letter, number or other characters such as '@'
  - changed every 2 months as a minimum
  - private to you and not shared with anyone else.
- Users under no circumstances should attempt to log in as a systems administrator.
- If a user identifies any kind of security issue with the Rendcomb College Network or the Internet. The user must notify the IT department immediately, and not demonstrate the problem to another user.
- Users should never attempt to circumvent the College's security measures via port scanning, tunnelling, proxy avoidance or any other means, to discover holes in the firewall.
- Users are responsible for preventing the spread of viruses and other destructive programs such as batch files. Emailing them around is strictly forbidden.

If a user is suspected to be acting outside the Acceptable Use Policy, a request for disclosure to monitor electronic behaviour will be approved by the Second Master in the Senior School or Head of the JS. Any resulting disciplinary procedures will be applied by the appropriate member of staff.

## Vandalism and Harassment

No users must ever intentionally attempt to vandalise Rendcomb IT equipment, and/or harass others, with examples being:

- An attempt to harm, modify or destroy data of another user, the Rendcomb network, and the Internet in accordance with the Computer Misuse Act.
- Transmitting or creating malware via the Rendcomb network or Internet.
- Attempting to harm, modify or destroy hardware, devices and software that belong to Rendcomb College, staff or pupils.
- Attempting to disrupt the Rendcomb network and/or Internet.
- Disrupting the work of other users or denying services to others (for example, by deliberate or reckless overloading or disabling of equipment).

Rendcomb College regards the following as harassment:

- Persistent annoyance of another user.
- Interference with another user's work.
- Sending or forwarding of unwanted email or malware/batch files as attachments.
- Posting inappropriate material or messages on social media, messaging apps or websites.
- Accessing another user's account and sending / forwarding inappropriate mail.

The Rendcomb College Network and Internet connection must not be used to break any relevant UK laws, regulations or policies or in a way that could disrupt access for other users. This includes:

- Unauthorised access to the network, servers, software, internet, facilities and data.
- Misuse of the Rendcomb College network, Internet and resources.
- Creation or transmission of any offensive or obscene media, messages or material.
- Creation or transmission of material that may cause annoyance, inconvenience or anxiety.
- To promote extremism organisations, extremist views or resources.
- Creation or transmission of material with the intent to defraud or infringe copyright.
- Creation or transmission of unsolicited bulk or marketing material unless the recipient has specifically requested it.

## Filtering & Monitoring

Schools in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*". Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education' in May 2016 for schools and colleges in England. Amongst the revisions, schools are obligated to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

Internet access is filtered for all users, but differentiated internet access is available for staff and customised filtering changes are managed by the school. It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision. The school will therefore monitor the activities of users on the school network and on school equipment whereby the monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum".*

We have ensured that appropriate filters and monitoring systems are in place to manage the content available to pupils, who can contact our pupils and the personal conduct of our pupils online. While it is acknowledged that filtering within our network is important, it does not help with regards to 3G and 4G, which give unrestricted access to the internet. Currently we are fortunate that given our remoteness, it is still quite difficult to access 3G/4G and even if you are able to, it is extremely slow, which effects the ability to stream videos and other digital content. However, we realise that it is important that we monitor this as technology changes rapidly. To help in this endeavor, we use https://360safe.org.uk/. At Present Pupils in College may carry mobile phones with them during the school day but these should only be used with the express permission of a member of staff. Boarders in Godman will be required to hand in their phones over night to ensure pupils cannot use 3G or 4G networks. Pupils in Lawn House, Stable House and Park house are allowed to keep phones with them, however this is at the discretion of the House parents and they will be removed if house staff feel they are being used inappropriately.

The College's policy on the use of mobile phones and cameras in the College, including the EYFS setting, is as follows:

There are separate acceptable use policy for the Senior School and Junior school. In the EYFS setting, neither staff nor pupils are permitted to bring mobile phones or any mobile device with a camera facility into the area. Staff and volunteers should use mobile phones and cameras in accordance with the guidance set out in the staff Code of Conduct.

Parents may bring mobile phones onto the premises but may only take photographs during events such as plays, concerts or sporting events for personal use. Parents should be reminded that the publications of such images (including on personal social networking sites even where access to the image may be limited) may be unlawful.

### Controversial Material

All users are responsible for the contents of their machine, including any illegal material found under their profile regardless if they were using the profile or not, including anything downloaded from the Internet.

All users should report any controversial material they find to the IT Department for removal. The IT Department will remove the material if it is appropriate to do so. Controversial material includes the list of items above in the vandalism and harassment section and any other inappropriate material including any resulting from activity which is illegal under UK Law. Pupils should also be aware of their obligation to report any activity or evidence that promotes extremism, in line with the PREVENT guidelines. More information can be found on the Safeguarding section of Firefly. Any concerns should be reported to the Designated Safeguarding Lead, their Deputy and network manager so appropriate steps can be taken as quickly as possible.

Rendcomb College assumes no responsibility for the content of websites over which it has no control. The School attempts to minimise access to inappropriate, malicious or offensive material. Rendcomb College will not be responsible for unauthorised financial obligation resulting from access to the Internet through the Rendcomb Network.

### Network Communication and File sharing

File sharing via peer to peer (P2P) networks of any kind on the Rendcomb College Network and internet is strictly forbidden. This includes but is not limited to:

- File sharing via Peer to Peer (P2P) networks or removable hard drives
- All file sharing or torrenting software
- Web sites designed to share files e.g. MegaUpload
- Create a sub network or domain

Users are also forbidden from trying to circumnavigate the Rendcomb College internet filtering system. This includes but is not limited to:

- Server devices and software
- Router software and devices
- Proxy software, websites and devices
- Devices and software intended to hide the identity of the device and/or user
- Devices and hardware intended to extract or eavesdrop on the network

### Use of Email

The following guidelines cover the use of Electronic Mail on the Rendcomb College Network, and through it to the Internet:

- Personal use of email is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason. All email can be recorded and stored, along with the source and destination.

- Write all messages and emails in correctly formatted English. Proof read everything.
- You must not send or forward chain emails, 'spam', malware or batch files.
- You must not forge emails or post anonymous messages
- Email is not something that can be regarded as being private. Think before you send!
- The use of extremist, racist, sexist, threatening or otherwise discriminatory and objectionable language in email messages is strictly forbidden.

### Plagiarism

Users should take care when using the internet to research information for academic work. Plagiarism is a breach of school and examination board rules and can involve liability for copyright infringement. Passing off another's work as their own will be classed as plagiarism and a breach of school rules.

### Network Etiquette (Netiquette)

Network Etiquette describes what is expected of a user, whilst using the Rendcomb College network and internet. This includes but is not limited to, the following:

- Be polite – treat others as you would want to be treated
- Do not send abusive or derogatory messages to anyone
- Respect other people's privacy, particularly on social media
- Do not give out personal information about yourself or other students/staff
- Minimise the use of acronyms (e.g. OMG, BTW)
- Don't engage in activities that are prohibited under UK law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden, as is any threatening, bullying or obscene matter.
- Don't take part in, or promote, websites or online groups/chats that encourage extremist activities.

### Software, Music and Video Copyright

The Rendcomb College IT department, have to abide by licensing law. All software installed on the Rendcomb College Network belongs and is licenced to Rendcomb College. Strict policies are in place to prevent pupils and non-IT staff from installing software. Under no circumstances should you attempt to install software of any kind or copy films and music to the network.

The College does not condone the unlicensed copying or use of software illegally. The liability for violating copyright in such cases is likely to rest with the individual concerned.

### Personal Data

Rendcomb College cannot accept responsibility for loss of data from your personal computer, whatever the cause. You are strongly advised to use Firefly's Personal Section for the storage of your studies-related data, allowing you to make use of our secure backup facilities.

Excessive storage consumption will be monitored with unnecessary media periodically removed.

**Confiscation, Search & Deletion**

Staff are authorised to confiscate electronic devices, examine any data on the device if they think there is a good reason to do so. (i.e. the staff member reasonably suspects that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules). The initial examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident.

Following an examination of an electronic device, if the member of staff has decided to return the device to the owner, they may ask the pupil to erase any data or files, if they think there is a good reason to do so. If however the member of staff decides to retain the device since the content is of a more inappropriate nature, they must inform the pupil that they are passing the matter (and device) over to the Second Master in the Senior School or Head in the JS. Depending on the content a decision will be made to delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

**Sanctions**

Any breach of these guidelines may result in disciplinary action under the school's disciplinary procedures by the Second Master, in the Senior School, or by the Head of the Junior School.

All users of the Rendcomb Network are responsible for respecting UK and international law. In the event of any action by proper authorities against any user, Rendcomb College will fully comply with the authorities to provide any information necessary for investigation and compliance.