Acceptable Use Policy

Acorn House College

Authorised by	**The principal and the proprietor**
Date	**December 2015**
Effective date of the policy	**February 2016**
Circulation	**Teaching staff, all other staff, volunteers, parents and students (on request)**
Last review date	**June 2018**
Next review date	**June 2019**

Contents

ACCEPTABLE USE 3
Scope 3
Aims 3
Internet and e-mail 3
What do Google Apps for Education include? 4
Protocols 5
Procedures 5
Students and the Law 6
The Data Protection Act 1984 and 1988 6
Copyright law 6
Whistle blowing and safe reporting 7
Sanctions 7
The liability of the College 7
Monitoring and review 7
APPENDICES 9
Appendix 1: Internet and e-mail protocol introduction 9
Appendix 2: Mobile electronic devices protocol 12
Appendix 3: Protocol for communication between staff and students 13

ACCEPTABLE USE

Scope

This policy has been authorised by the Principal and is addressed to all students (with staff to take due regard). It covers all sections of the college. It is available to parents on request and parents are encouraged to read it. This policy relates to the use of technology, including:

- the internet
- e-mail
- mobile phones and smartphones
- computers, be they desktops, laptops, netbooks, chromebooks, tablets or other such devices
- personal music players
- devices with the capability for recording and / or storing still or moving images and/or audio
- social networking, micro-blogging, blogs, message boards and other interactive web sites
- instant messaging, chat rooms and other similar communication services
- webcams, video hosting sites (such as YouTube)
- gaming sites
- other photographic or electronic equipment
- wearables, such as Apple iWatches.

It applies to the use of any of the above on College premises and also any use, whether on or off College premises, which affects the welfare of other students or where the culture or reputation of the College are put at risk. Staff are subject to a range of separate detailed policies to cover the use of technology and working safely more generally, but should pay due regard to this policy.

Aims

The aims of this policy are:

- to encourage students to make good use of the educational opportunities presented by access to the internet and other electronic communication;
- to safeguard and promote the welfare of students by preventing cyberbullying, access to radicalisation and other forms of abuse;
- to minimise the risk of harm to the assets and reputation of the College;
- to help students take responsibility for their own e-safety (i.e. limiting the
- risks that students and young people are exposed to when using technology);
- to ensure that students use technology safely and securely.

Internet and e-mail

The College provides internet access and an increasing suite of tools based on Google Apps for Education, to students to support its academic activities and to maximise the educational opportunities presented by such access. This includes an e-mail system, unlimited storage of ‘cloud-based’ file and documents storage and access to “google classroom” which is a powerful file sharing and collaboration tool.

Students may only access the College's network when given specific permission to do so. All students will receive guidance on the use of the College's domain, internet and e-mail systems. If students are unsure about whether you they doing the right thing, they must seek assistance from a member of staff.

For students' own protection and that of others, use of the college's domain, e-mail and of the internet will be monitored by the College. **Even when an email or downloaded document or file has been deleted, it can still be traced on the system**. Students should not assume that files stored on servers or storage media are always private.

In our undertaking with our service provider for Google Apps for Education, we confirm that no students under the age of 13 will have access to services that require a 13+ age requirement. Should students under the age of 13 compromise their account by accessing services then Google will freeze their account and all materials and files therein. The College has no ability to influence Google actions should this happen. Students/Students must enter their true date of birth when/where requested.

We make use of Google Apps for Education to provide many of our digital services on-line. Google Apps represents an important step toward developing a 21st century approach to curriculum and learning. We have built these various tools and services around a college domain (acorn-college.co.uk). This domain provides a closed 'walled garden' within which our college teachers and students can work, share and collaborate, and to which external individuals do not have access unless the internal users choose to share with external users. The college has a firewall in place to restrict access to certain sites via the College's wifi network. This policy is designed to cover internet access from this network and any other network, including 3G and 4G cellular networks whether on or off the College premises.

What do Google Apps for Education include?

- Students will be given a specific e-mail address by the College administrator. E-mail will be used for college-related purposes and will be used when sharing documents and collaborating.
- Google Calendar allows students to create and share college or class calendars and events.
- Google Drive provides unlimited cloud-based storage for each account.
- Google Docs lets students create and share documents, spreadsheets, presentations, drawings and forms. They will be able to upload any file to Google Docs and share it with others, including external users if/as appropriate.

- Google Sites make it easy to collect, share and publish all types of content in a single website through the easy embedding of Google Docs, Calendars, videos and other media.
- Also included are Google Groups for mailing lists, discussion groups, and broad sharing, Google video for domain-limited video distribution, as well as other tools that can be added onto the domain. Our IT systems administrator will determine if and when other products will be released into the domain, after consultation with academic colleagues.
- Google Apps continue to expand their areas of interest and application. Acorn House College will continue to expand that offer to our community as the opportunities arise, such as Google Classroom, but do not always make available all tools for the use of students.

Protocols

Students should comply with the following protocols:

- Domain, internet and e-mail protocol (Appendix 1);
- mobile electronic device protocol (Appendix 2);
- protocol for communication between staff and students (Appendix 3)

Procedures

- Students are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and legal. Any student who becomes aware of misuse by other students should talk to a teacher about it as soon as possible.
- Any misuse of the internet will be dealt with under the College's Behaviour and Discipline Policy.
- Students must not use their own or the College's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the College's Anti-bullying Policy. If a student thinks that he/she might have been bullied or if he/she thinks another person is being bullied, the student must talk to a teacher about it as soon as possible. Please refer to the College's Anti-bullying policy.
- Current behaviours that fall into this category, often referred to as Cyber-bullying include:

- Texting scary or rude messages by mobile phone
- sending unpleasant photographs by mobile phone
- using online message boards, chat rooms or social networking sites to post cruel messages
- deleting the victim's name from or ignoring their messages on social networking sites

Someone taking an indecent image of themselves, and sending it to their friends or boy/girlfriend via a mobile phone or some other form of technology is sometimes referred to as 'sexting'. **The creation, possession and transmission of any indecent image containing a person under 18 is illegal, and the college is required to report such incidents to the police.**

Once these images have been taken and sent to others, control is lost of them and they can end up anywhere. They could be seen by friends and family, a future employer, or even, in some cases, end up in the possession of an offender.

This also puts the person who originally sent the images in a vulnerable position, as somebody they may or may not know now has these images and could use technology to bully, harass or even try to locate them.

Our advice to young people is:

- **"Just think – if you wouldn't print and pass these images around your college or show your mum or dad, they are not appropriate to share via phone or other technologies."**

Students should also remember that any material posted online can potentially remain there to be found indefinitely. The BBC and other websites have good coverage of the various news stories that cover serious incidents arising from cyber-bullying. A good example for 11-16 is the http://www.thinkuknow.co.uk/11_16/ site.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the College's child protection procedures (see the College's Safeguarding/Child Protection Policy). If a student is worried about something seen on the internet, they should talk to a teacher about it as soon as possible.

Students and the Law

Computer Misuse, Data Protection, Copyright, Whistle blowing and Safe reporting. In this section 'you' covers both students and adults.

- You may not access computer material without permission, eg looking at someone else's files.
- You may not access computer material without permission with intent to commit further criminal offences, eg *hacking* into the bank's computer and wanting to increase the amount in your account.
- You may not alter computer *data* without permission, eg writing a *virus* to destroy someone else's data, or actually changing the money in an account.

The Data Protection Act 1984 and 1988

This helps to provide protection against the abuse of personal information. You may not collect data without planning to use it sensibly, within reason and store it safely.

Copyright law

You are not allowed to misuse other people's creative work, such as by the copying of written, musical, or film work using computers. During our teaching, students will learn how to find and use a variety of copyright free and licensed resources. In work students create for exam boards, they must be very careful to quote all sources and references.

Whistle blowing and safe reporting

If you are a victim of computer abuse or witness others who are victims of abuse, we want you to speak out. You can do so by speaking to an adult or teachers. You can also speak about an adult and/or teachers at the College Office, or by emailing info@acornhousecollege.com If you feel you cannot speak to someone in College, then please contact external agencies such as Childline 0800 1111 or message them at www.childline.org.uk. Other organisations such as the Safe network - http://www.safenetwork.org.uk exist to ensure that appropriate safeguarding information and resources are made available to keep students and young people safe and to assist in making an independent visitor aware of your concerns.

Sanctions

Where a student breaches any of the College's protocols, the Principal has authority to apply any sanction which is appropriate and proportionate to the breach in accordance with the College's Behaviour and Discipline Policy including, in the most serious cases, expulsion. Other sanctions might include:

- increased monitoring procedures, withdrawal of the right to access the College's domain, internet and e-mail facilities and detention. Any action taken will depend on the seriousness of the offence.
- Unacceptable use of electronic equipment could lead to confiscation in accordance with the protocols attached to this policy and the College's Behaviour and Discipline Policy.
- The College reserves the right to charge a student or his / her parents for any costs incurred to the College, or to indemnify any significant liability incurred by the College as a result of a breach of this policy.

The liability of the College

Unless negligent under the terms of this policy, the College accepts no responsibility to the student or parents caused by or arising from a student's use of the internet, e-mail or any electronic device whilst at College. Parents choosing to enable iTunes or Google Play on their child's device do so at their own risk. These features require the user to log credit card details to enable the Apps (even if free) to be installed. The College does not undertake to provide continuous internet access. E-mail and website addresses at the College may change from time to time.

Monitoring and review

All serious e-safety incidents will be logged in the Incident Book.

The Principal, in consultation with other staff members, has responsibility for the implementation and review of this policy, in consultation with parents, students and staff. The Principal will consider the record of e-safety incidents and new technologies and will consider if existing security procedures are adequate. The College advisers with responsibility for Safeguarding and Child Protection (The principal) will make an annual report to the Governors on the effectiveness of the College's Acceptable Use Policy and associated procedures.

APPENDICES

Appendix 1: Internet and e-mail protocol introduction

We want each student to enjoy using the internet, and to become proficient in drawing upon it both during their time at College, and as a foundation for further education and future careers. However, there are some potential drawbacks with e-mail and the internet, both for students and for the College. The purpose of this protocol is to set out the principles which you must bear in mind at all times and also the rules which you must follow in order for all students to use the internet safely and securely. The principles and rules set out below apply to all use of the internet, including social media, and to the use of e-mail in as much as they are relevant. Failure to follow this protocol will constitute a breach of discipline and will be dealt with in accordance with the College's Behaviour and Discipline Policy.
The IT systems administrator can be contacted through netadmin@acorn-college.co.uk

Access and security
Access to the internet from the College's computers and network must be for educational purposes only. You must not use the College's facilities or network for personal, social or non-educational use without the express, prior consent of an appropriately competent member of staff.

You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the College's or any other computer system, or any information contained on such a system.

No laptop or other mobile electronic device may be connected to the College network without the consent in writing of the IT Systems administrator. The College operates a wireless filtered password-protected service for all students (wifi), which they can access using their own phones, tablet or laptop.

Students seeking permission to use the wifi on such devices are welcome to do so but must remember that they are restricted to use for the purposes identified in this policy

Students should only connect personal devices to the wifi. They should not make use of 3/4G connectivity, which bypassess our filtering system. They should not piggyback onto the college’s network cabling/sockets without express permission. It should be noted that traffic travelling through the college Internet connection will be intercepted and logged. This may also apply to data sent securely (via HTTPs).

College staff will NOT provide technical support and peripheral equipment. Students who are not doing academic work or are creating a disruption will be asked to put the device away. Students should make sure they have adequate insurance for their devices including accidental damage cover that protects them in college. The college cannot be held responsible for any damage or loss of devices.

Passwords protect students own accounts within Google Apps for Education as well as the College's network and computer system. Students should disclose their passwords. If a student believes that someone knows their password it must be changed immediately.

Students should not attempt to gain unauthorised access to anyone else's computer, domain account or to confidential information which you are not authorised to access. If there is a problem with a password, please speak to an administrator or the principal

The College has a firewall in place to ensure the safety and security of the College's networks. Students must not attempt to disable, defeat or circumvent any of the College's security facilities. If students notice a problem with the firewall, they should speak to an administrator or the principal immediately. Viruses can cause serious harm to the security of the College's network and that of others.

Viruses are often spread through internet downloads or circulated as attachments to e-mails. If students think or suspect that an attachment sent to them, or other material such as that available for download, might contain a virus, they must speak to a teacher before opening the attachment or downloading the material. Students must not disable or uninstall any anti-virus software on the College's computers.

Use of the internet
Students must use the College's computer system for educational purposes only.

Students must take care to protect personal and confidential information about themselves and others when using the internet, even if you receive or come across this information inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.

Students must not load material from any external storage device (such as USB drives) brought in from outside the College onto the College's systems, unless this has been authorised.

Students should assume that all material on the internet is protected by copyright and must treat such material appropriately and in accordance with the owner's rights - students must not copy (plagiarise) another's work. Wherever possible, and as directed by the teachers, students should make appropriate reference in working documents to any external sources from where they have gained copyright material for personal use.

Students must not bring the College into disrepute through your use of the internet.

Viewing, retrieving, downloading or sharing any material which in the reasonable opinion of the Principal is unsuitable, at any time, is strictly prohibited. Students must tell a member of staff immediately if you have accidentally read, downloaded or have been sent inappropriate material, including personal information about someone else.

Students must not enter into any contractual commitment using the internet when in the care of the College, or otherwise associated with the College, whether for themselves or on behalf of another (including the College). Students will support the college's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the college or wider community.

Use of e-mail

Student e-mail accounts come as part of the Google Apps for Education service and is a private gmail account that should be used only to communicate with other members of the College community. gmail is encrypted, so sensitive data can be sent via gmail, but we urge caution about this.

Students must not use any personal web based e-mail accounts such as Yahoo or Hotmail through the College's network. This will be unnecessary as you are provided with your own personal g-mail account for College purposes. College e-mail accounts can be accessed from home by logging in via gmail account, and accounts are usually available throughout the calendar year. E-mail should be treated in the same way as any other form of written communication. Students should not include or ask to receive anything in an e-mail which is not appropriate to be published generally or which you believe will be seen as inappropriate for a student at the College.

Students must not send, search for or receive any e-mail message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If unsure about the content of a message, students should speak to a member of staff. If students come across such material they must inform a member of staff as soon as possible. Use of the e-mail system in this way is a serious breach of discipline. The College will take no responsibility for any offence caused as a result of downloading, viewing or forwarding inappropriate e-mails

Trivial messages and jokes should not be sent or forwarded through the College's e-mail system. Not only could these cause distress to recipients (if inappropriate) but could also cause the College's IT system to suffer delays and / or damage.

All correspondence from your College e-mail account must contain the College's disclaimer.

Students must not read anyone else's e-mails without their consent.

Appendix 2: Mobile electronic devices protocol

Use of mobile electronic devices "Mobile electronic device" includes without limitation mobile phones, smartphones, tablets, laptops, MP3 players.

A student's mobile phone should be protected by either a password or 'gesture' to prevent unauthorised access. Users/parents need to be aware that remote location and wiping are possible for both Android (https://www.google.com/android/devicemanager) and iPhones (iCloud)

Students may not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Principal.

The College does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto College premises, including devices that have been confiscated.

Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline, whether or not the student is in the care of the College at the time of such use. Appropriate disciplinary action will be taken where the College becomes aware of such use (see the College's Anti-bullying Policy and Behaviour and Discipline Policy.

The College reserves the right to confiscate a student's mobile electronic device for a specified period of time if the student is found to be in breach of this protocol. The student may also be prevented from bringing a mobile phone into the College temporarily or permanently and at the sole discretion of the Principal.

Photographs and images
Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

Students may only use cameras or any mobile electronic device with the capability for recording and / or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.

All students must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.

The posting of images which in the reasonable opinion of the Principal is considered to be offensive on any form of social media or websites such as Youtube, Facebook, Snapchat etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using College or personal facilities.

Appendix 3: Protocol for communication between staff and students

Acorn House College is committed to safeguarding and promoting the welfare of students at the College. As part of our safeguarding policy we expect staff and students, and where appropriate, parents, to follow this protocol on communication by mobile phone. Throughout this protocol the term mobile phone includes a tablet or similar device.

On college premises
Phones must not be used during lessons unless the teacher has asked students to do so as part of the lesson. Telephone numbers must not be exchanged on the premises. Any messages that are sent must be brief and courteous. Staff must not correspond with students via text message or other messaging services unless via college-owned devices and for a specific, college-related purpose.

Phones should be used only when necessary and should not cause a disruption or nuisance to anyone at the College. If a member of staff asks a student to stop using their mobile phone the student must do so immediately and risks having the device confiscated if they continue using it or causing the disturbance.

Outside college
We appreciate that we cannot control messages sent between students when off the premises across other networks using personal devices, however we ask that students are mindful of this policy and of the College's anti-bullying and behaviour policies. Staff must not correspond with staff via text message or other messaging services unless via college-owned devices and for a specific, college-related purpose. If personal devices are used, message must be brief, courteous and for a specific, college-related purpose.

The leader of an educational visit will carry a mobile phone supplied by the College if appropriate, and, as part of the preparations for the visit, will ensure that other adults taking part in the visit are equipped with mobile phones (or digital walkie talkies) and that relevant numbers are exchanged.

Staff and students taking part in such visits must not use mobile phones to speak or send messages to each other except in emergencies or to provide essential information. Any messages that are sent must be brief and courteous. Staff managing sports teams and similar activities may use mobile phones or send messages to keep parents and other interested parties briefed for purposes of information, collection and supervision.

Inappropriate communications
If there are reasonable grounds to believe that inappropriate communications have taken place, the Principal will require the relevant mobile phones to be produced for examination. The usual disciplinary procedures will apply.

Students may expect to have mobile phones confiscated if there has been a breach of this protocol. Staff may expect to face disciplinary procedures as published by the Principal.

Students and staff must be conscious at all times of the need to keep personal and professional lives separate. You must not put yourself in a position where there is a conflict between your work for the college and your personal interests. This means for students that they must not use the same social media identities for college and private lives. At no stage should employees or students risk reputational damage to the college through inappropriate use of social media

Staff employees must decline 'friend requests' from students, which they receive on their personal social media accounts. Instead, if they receive such requests from students who are not family members, they must discuss these in general terms in class.

Photographs, videos or any other types of image of students and their families, or images depicting staff members appearing in association with the College wearing college or images identifying sensitive college premises must not be published on a student's personal webspace. Parents and students must be especially careful about publishing on their family spaces pictures of other students in the college, unless they have the express permission of the students and families involved. 'Facebooking' images shared with families of students by teachers to demonstrate progress made or successes achieved is not permitted.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be embarrassing if too much personal information is known in the workplace.

As the College introduces the students to e-learning, in many instances, the required way of working will be digitally. However, this does not mean that by default, students may opt to work on their personal laptop rather than use paper or other directed ways of working.

If a student wishes to work in class with a device such as laptop or tablet, he / she must obtain the express permission of their parents and the class teacher.

The following is also presumed:

- there is identified need because of SEN or other needs, by SENCo or Educational Psychologist, or there is an academic need or value identified by the teacher of doing so
- the student has their own device, or in extremis the College has the resources to loan such a device. The electronic device must be adequately marked and insured by the student/parent.
- the use of the laptop will not interfere with the learning of that student or of others and will not slow down the pace of the lesson eg if the student has a slow typing speed

- the College will have procedures in place to monitor the student's effectiveness as a laptop user, to provide appropriate support for the coaching of new skills and the management of appropriate paper record or work for their teachers
- In exceptional circumstances, the College can insist that a student works on a laptop, because the legibility of their writing or their productivity are inadequate to ensure assessment & evaluation of progress can take place
- In addition, a student may use a laptop or other electronic device on a temporary basis if necessary as a result of a temporary condition caused by illness or injury.
- Student and parents have agreed to comply with this Acceptable Use of ICT policy

.