# HGCS TECHNOLOGY ACCEPTABLE USE POLICY (AUP)

## OVERVIEW

The Hickory Grove Christian School Acceptable Use Policy (AUP) document was created to outline and define the acceptable use policies and expectations of the students as they are relevant to the use of technology both on and off campus.

Hickory Grove Christian School (HGCS) uses technology as a method to deliver education to the student. HGCS recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. Today's technology is an essential component of expanding the student's mind and we are committed to helping students develop technology and communication skills. To that end, our goal is to provide a safe and secure access to technologies for student and staff use.

Network access carries certain responsibilities and obligations as to what constitutes acceptable use of the HGCS network. The Internet is a resource that contains instructional value, and when used properly, can offer the end user infinite educational resources. These policies explain how HGCS information technology resources are to be used and specify what actions are prohibited. While this Acceptable Use Policy may be thorough, no set of policies can cover every situation, and thus, the user is asked to additionally use sensible judgment when using HGCS technology resources. Questions on what constitutes acceptable use should be directed to the grade level principals.

## PURPOSE

The purpose of these policies is to detail the acceptable use of HGCS information technology resources for the protection of all parties involved.

## SCOPE

These policies apply to any and all use of HGCS IT resources including, but not limited to, computer systems, personal mobile devices, email, network, and the HGCS Internet connection.

## E-MAIL USE

Personal usage of HGCS email systems is permitted as long as A) such usage does not negatively impact the HGCS computer network, and B) such usage does not negatively impact (bully, harass, etc.) parties involved.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to HGCS may not be sent via email, regardless of the recipient, without proper encryption.
- The user should not attempt to circumvent security or filtering systems.
- It is HGCS protocol not to open email attachments from unknown senders or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.
- Language in emails should be appropriate and not contain profanity.

## CONFIDENTIALITY

Confidential data must not be A) shared or disclosed in any manner (this includes, but is not limited to, providing or receiving a student's username and password used to access secured areas such as learning management systems, grade reporting systems, websites, applications, etc.), B) posted on the Internet or any publicly accessible systems, or C) transferred in any insecure manner. It is dangerous to disseminate personal information (full name, address, DOB etc.) in an online setting.

## NETWORK ACCESS

The user should take reasonable efforts to avoid accessing network data, files, and information that are not applicable to them. Existence of access capabilities does not imply permission to use this access. Additionally, HGCS is not responsible for data loss on HGCS devices.

# HGCS TECHNOLOGY ACCEPTABLE USE POLICY (AUP) CONTINUED

## UNACCEPTABLE USE

The following actions shall constitute unacceptable use of the HGCS network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the HGCS network and/or systems to:

- Engage in activity that is illegal under local, state, federal, international, or other applicable laws.
- Engage in any activities that may compromise biblically moral standards, cause embarrassment, loss of reputation, or other harm to HGCS.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the learning environment.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques.
- Install or distribute unlicensed or "pirated" software.
- Engage in activity that could harm the network and/or computer devices (virus).
- Stream music or play executable computer games.

## WEB BROWSING

The Internet is a network of interconnected computers of which the district has very little control. The user should recognize this when using the Internet and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. Although a filter is in place, it is impossible to block every site that may be deemed offensive. The user must use the Internet at his or her own risk. HGCS is specifically not responsible for any information that the user views, reads, or downloads from the Internet. Additionally, HGCS is not responsible for the accuracy and/or quality of information obtained from the Internet. HGCS recognizes that the Internet can be a tool that is useful for both personal and professional purposes.

## COPYRIGHT INFRINGEMENT

HGCS's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of the acceptable use policy if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CDs and DVDs, B) posting or plagiarizing copyrighted material, and C) downloading copyrighted files which the user has not already legally procured. This list is not exhaustive; copyright law applies to a wide variety of works and applies to much more than is listed above.

## PEER-TO-PEER FILE SHARING

Peer-to-Peer (P2P) networking is not allowed on the HGCS network under any circumstance.

## STREAMING MEDIA

Streaming media can use a great deal of network resources and is prohibited.

## EXPECTATION OF PRIVACY

Users should expect no privacy when using the HGCS network. Such use may include but is not limited to, transmission and storage of files, data, and messages. HGCS reserves the right to monitor any and all use of the computer network. To ensure compliance with district policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

## BANDWIDTH USAGE

Excessive use of HGCS bandwidth or other computer resources is not permitted.

# HGCS TECHNOLOGY ACCEPTABLE USE POLICY (AUP) CONTINUED

## CIRCUMVENTION OF SECURITY

Using HGCS-owned computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited. If an individual is aware of someone circumventing security and/or demonstrating this to others the individual should immediately alert the school principal or faculty.

## SOFTWARE INSTALLATION

Numerous security threats can masquerade as innocuous software - malware, spyware, and trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. Therefore, HGCS approved software will be installed on applicable computers determined by the System Administrator.

## ILLEGAL ACTIVITIES

No HGCS-owned computer systems may be knowingly used for activities that are considered illegal under local, state, federal, international, or other applicable laws. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material
- Downloading, storing, or distributing or unauthorized streaming of copyrighted material

HGCS will take all necessary steps to report and prosecute any violations of these policies.

## CYBER-BULLYING

Harassing, denigrating, impersonating, pranking, excluding, and cyber-stalking are all examples of cyber-bullying. Cyber-bullying will not be tolerated. Sending emails or posting comments, images, and/or other content with the intent of scaring, hurting, or intimidating someone else can be considered cyber-bullying.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, can be a crime. These behaviors may also result in severe disciplinary action and loss of privileges. Remember network activities are monitored and retained.

## SECURITY/SAFETY

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

# HGCS TECHNOLOGY ACCEPTABLE USE POLICY (AUP) CONTINUED

## PARENT/GUARDIAN RESPONSIBILITIES

It is strongly suggested that parents communicate with students about values and the standards they should follow regarding the use of the Internet and all media information sources such as television, cell phones, electronic devices, videos, movies, and music.

## APPLICABILITY OF OTHER POLICIES

This document is part of a cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

## AUDITS

HGCS will conduct periodic reviews to ensure policy compliance. A sampling of users will be taken and audited against these policies on a random basis.

## ENFORCEMENT

The IT Department and/or Executive Team will enforce these policies. Violations may result in disciplinary action, which may include suspension, restriction of access, or other punishments deemed appropriate by HGCS executive personnel. Where illegal activities or theft of school property (physical or intellectual) are suspected, HGCS may report such activities to the applicable authorities.

## REVISION HISTORY

Revision 1.1 7/06/2017
Revision 1.0 7/14/2015

Parent Signature Date

Student Signature Date

# GOOGLE AGREEMENT FOR COLLECTION OF DATA

To parents and guardians,

At Hickory Grove Christian School, we use G Suite for Education, and we are seeking your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. At Hickory Grove Christian School, students will use their G Suite accounts to complete assignments, communicate with their teachers, sign into their Chromebooks, and learn 21st century digital citizenship skills.

The notice below provides answers to common questions about what Google can and can't do with your child's personal information, including:

- What personal information does Google collect?
- How does Google use this information?
- Will Google disclose my child's personal information?
- Does Google use student personal information for users in K-12 schools to target advertising?
- Can my child share information with others using the G Suite for Education account?
- Please read it carefully, let us know of any questions, and then sign below to indicate that you've read the notice and give your consent. If you don't provide your consent, we will not create a G Suite for Education account for your child.

I give permission for Hickory Grove Christian School to create/maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice below.

Thank you,
Dr. Jimmie Quesinberry

Full name of student

Printed name of parent/guardian

Signature of parent/guardian Date

# GOOGLE USE AGREEMENT

Our G Suite for Education Privacy Notice describes how Google products and services collect and use information when used with G Suite for Education accounts.

Information about the legal commitments Google makes for G Suite for Education Core and Additional Services is available in our Help Center.

Information about how Google's products work to protect privacy is available in our Product Privacy Guide and at privacy.google.com. Note that Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads for G Suite for Education users in primary and secondary (K–12) schools, and any statements about ads on those pages are overridden by this restriction from our Privacy Notice.

Information about Google's compliance with international legal obligations on data protection can be seen in the Data Processing Amendment to G Suite and/or Complementary Product Agreement, which describes extensive measures for data security that Google and its customers have agreed.

Answers to many top questions about privacy and security appear on our Google for Education Trust page.
Parents can visit myaccount.google.com while signed in to their child's G Suite for Education account to view and manage the personal information and settings of the account.