BISHOP GARCIA DIEGO HIGH SCHOOL

INTERIM ACCEPTABLE USE POLICY

2018-2019

Table of Contents

DEFINITIONS[1]

Knowledge of the following definitions is important to understanding the Acceptable Use Policy (the "AUP").

access any action that may be taken to open and read data from a Record or Software including connecting, linking, or attaching to a Resource; the reading or writing of data to/from memory

Account consists of a User's name, an assigned User ID, a password, and other information necessary to keep track of a User on Bishop Resources

Activity Data data automatically generated by use of Bishop Resources including records of Internet use and web-sites visited, and logs of access to Bishop Diego facilities, accessible from Bishop Resources maintained by Bishop Diego or its agents

All Records refers to both Bishop Records and Personal Records (see "Records")

Authorized Administrator an official, administrator, or supervisor who is authorized to approve access and activities with respect to Bishop Resources and make decisions regarding issues arising under the AUP

Bishop Diego Community students who have enrolled at Bishop Diego (i.e., accepted an offer to enroll and made the required deposit), their parents and relatives; employees under contract including Faculty, staff, clergy, members of religious orders, facilities personnel; volunteers, alumni, donors and benefactors; and vendors, general contractors, subcontractors who are under an executed but not fully performed contract to provide services or goods—whether on or off-campus

Board the Board of Trustees of Bishop Diego High School

campus all land and buildings owned or leased by Bishop Diego high school at 4000 La Colina Rd., Santa Barbara, CA

[1] Definitions are from the Electronic Communications Privacy Act, 18 USC § 2510(12) (1986); Barron's Dictionary of Computer and Internet Terms (Ed. Douglas Downing, PH.D., 2017), Webster's New World Computer Dictionary (Ed. Bryan Pfaffenberger, 10th Ed. 2003), and; Merriam-Webster's Online Dictionary (https://www.merriam-webster.com/) accessed in May and June of 2018.

cloud, cloud computing where a company, organization, institution or enterprise relies on and accesses remotely a set of computers belonging to a third-party service provider for servers, Software (including applications), and storage

Cloud Based Storage any cloud-based system capable of recording, storing, or retrieving Records, Software, Electronic Information, or electronic communications including internet-based storage and backup including Drop Box, Box, OneDrive, Google Drive, Sky Drive, iCloud, Amazon S3, Carbonite Online Backup, EMC's Mozy, EVault, Iron Mountain Digital, Symantec Online Backup and SPN

component any part or module of a larger system

computer a machine capable of executing instructions on data, i.e., that can follow instructions to alter data or perform tasks/operations without human intervention by representing and manipulating text, numbers, graphics, symbols, and music, with the distinguishing feature of the ability to store its own instructions

Confidential Records any Bishop Record which is classified by Bishop Diego as either confidential or internal-use-only Information

content - the substance or meaning of electronic communications between two or more people such as the communications found in e-mails or other Records

data distinct, factual information—such as text, numbers, letters, images, sounds, graphics

database a collection of data/information; a database often, if not always, consists of a collection of records, subdivided into fields, with data input into each field

Device[2], Bishop Device any portable hardware, peripheral, or component which can transmit Records, Software, other Electronic Information, and other electronic communications including but not limited to portable computers, stand-alone computers (if brought to campus), laptops, tablets, notebooks, monitors, portable printers, photographic-, audio- and video-equipment, media players, multimedia equipment, scanners, copiers, regular/wired and

[2] For purposes of the AUP, the definition of "Device" is broader than the one typically found in dictionaries for "device" (a "component of a computer that is used for input or output, such as a printer, modem, disk drive. . . .") The intent is to capture within the definition all of the various types of personal electronic communications hardware that a student or other User might commonly bring on campus, including items that themselves would be considered a computer, and items that might not ordinarily be considered a "component" of a computer (e.g., cell-phone or pager).

mobile/wireless telephones, Blackberries, iPods, smart-phones, two-way radios, pagers, other wireless equipment, any device that can play digital audio files including MP3 players, and any other electronic communications hardware that may be created and used by Students, Faculty, and staff in the future; referred to as a "Bishop Device" if owned, leased or controlled by Bishop Diego

domain in a computer network, a group of computers that are administered as a unit

electronic communication any transfer or transmitting of data, signs, signals, writings, images, sounds, or intelligence of any nature transmitted in whole or in part by wire, wireless, radio, electromagnetic, photo-electronic, or photo-optical system including, for example, e-mail, SMTP, personal- and instant-messages (computer networks); texts (cell phone networks); voicemail, fax and pager (PSTN); and one-to-many communications such as bulletin boards, internet forums, and usernet (on computer networks)

electronic data data in an electronic form that can be processed by a computer

Electronic Information information in an electronic form that has been processed by a computer, usually if not always found in files, sometimes formatted for specific Software

enroll students are enrolled at Bishop Diego if they have signed an enrollment contract and made the required deposit

equipment the set of articles or physical resources serving to equip a person or thing such as the implements used in an activity, operation or system

execute to use or run Software, i.e., a program

Faculty both Teachers and administrative staff

file a block or collection of Electronic Information given a unique name called a filename, found on an IT Resource (System, Device, or Media) with storage capability; files may contain or constitute a document, message, e-mail, text message, instant message, posting on social media, or other electronic communication; a program, operating system, application such as a database, spreadsheet or web application; or an image, graphics, photograph, video, film, recording, song/music; it may include other electronic content, e.g., User Account information and Activity Data

folder a directory of files

forum an online service with topically focused discussion group that is supervised by a host or moderator, where parties may contribute their thoughts on various subjects and where such communication is made available for others to read and comment, such as a chat room, blog, e-mail, news-group, bulletin board, social networking website

Guest anyone who is not part of the Bishop Diego Community such as prospective students from a middle-school and their parents or relatives; prospective donors and benefactors; prospective vendors or contractors wishing to submit a bid on a project; members of the public on-campus for a tour, visiting an event, or loitering, or related to members of, or interested in, an opposing sports team visiting for a competition (including referees, students, parents, youth, children, teachers, coaches); guests can be found at off-campus events that are hosted by Bishop Diego (e.g., a luncheon or a sports event at Santa Barbara City College, etc.)

Guest Wireless Network an open, unsecured WiFi network provided on-campus that allows Guests temporary wireless access to the internet/World Wide Web only, and does not allow access to any other Bishop Resource

hack the unauthorized access, use, improvised modification, disclosure, re-programming, planting of a virus or breaking into, or theft of, a Resource, Record, or Program for gain, malice, mischief, or to prove it can be done (i.e., a security violation), including but not limited to:

1. cracking, penetrating or successfully evading: i) the security features of another User's Bishop Diego Account, or ii) other Bishop Diego security system,

2. accessing (including remote access) of Bishop or Personal Resources,

3. reviewing, scanning, modifying, or transmitting of a Bishop Record to a Personal Resource, or other theft of Bishop Records, including Bishop Diego logos, images, trademarks, or copyrighted materials,

4. showing or disclosing a Bishop Record or Personal Record to another User (e.g., students) on campus, or off-campus at events hosted by Bishop Diego or where members of the Bishop Diego Community are participating in an activity,

5. theft of a Bishop or Personal Device, Media or Record, or

6. copying or placing a Personal Record or Software, including a virus, spyware, malware, or trojan horse, onto a Bishop Diego or Personal Resource or Record.

hardware the physical elements of a computer system including boards, equipment, the computer, peripherals, and any electronic or electrical apparatus or component

information data—such as text, numbers, images, sounds or graphics—that has been organized, systematized, and presented in a usable form and pattern, so that the underlying patterns or phenomena become clear; knowledge obtained from investigation or study of data, e.g., a computer simulation that shows how data from hundreds of report cards predicts a likelihood of success in college is information

Legitimate School Reason refers to a specific school justification for an activity—educational, administrative, business, or other—approved by an Authorized Administrator

Media any portable optical, magnetic or solid-state equipment, hardware or object that is capable of storing or recording Records, Software, Electronic Information, or electronic communications including, but not limited to, CDs, DVDs, discs, laser discs, computer discs, external hard-drives, NAS devices, circuit boards, any type of portable storage device such as a flash drive aka USB- and jump-drive, thumb-drive, data stick, pen drive, keychain drive, or any other item with a similar function; referred to as a "Bishop Media" if owned, leased or controlled by Bishop Diego; stand-alone computers, networks and Cloud-based Storage are excluded from this definition

Modify, modification action that may be taken to affect or act upon a Record or Software including editing, altering, redacting, deleting in part or in whole, or any other change or disposition

Multimedia refers to a technology, a computer-based method of producing and presenting combined sound and visual product, content and information, to inform and/or entertain, by utilizing more than one content form/medium of communication such as audio, video, text, images, graphics, animations, emphasizing interactivity and interactive content; multimedia can be recorded and played, displayed, interacted with or accessed by information content processing equipment

Multimedia Equipment all of the computerized Systems, Devices and Media used to create, produce and experience live and recorded Multimedia product and performances

network a set of computers connected together; a communications, data exchange, and resource-sharing system created by linking two or more computers and establishing standards and protocols, so that they can work together

Notice of Third Party Request a notice that Bishop Diego sends to a User informing them that Bishop Diego has received, or been served with, a Request for Access to Records involving a Record, Software or other Electronic data or information related to the User

peripheral a device connected to and controlled by a computer but external to the computer's central processing unit, such as a printer or disk drive

Personal Identifying Information includes contact information such as name, work residence or school address, phone number, e-mail address, screen name, or web addresses (URLs) of forums

Personal Record a Record that is created, accessed, modified, transmitted or stored by a User for personal use that is not related to Bishop Diego's educational or Catholic mission, administrative, or business activities, was not created, accessed, modified, transmitted or stored on Bishop Diego's Bishop Resources, and is not related to Bishop Diego activities, student life, or implicates Bishop Diego in any way

Personal Resource a user-owned Device or Media which is dual-use in that it can be used for personal matters; and also for Bishop Diego activities such as student life, educational use, after-school homework or assignments, or teaching activities, business, administrative or other matters

Portable Device, Portable Media means a Device or Media that is easily transportable, and capable of accessing, transmitting or storing electronic information

program a set, list or sequence of coded instructions, i.e., written in a programming or assembly language, that a computer can execute performing pre-determined tasks usually, if not always, with data that is provided, generating new data and providing information, often in an organized, systematized way

Record, Bishop Record[3] electronic information that is related to Bishop Diego's educational mission, administration or business, or to Bishop Diego student activities or student life, or implicates Bishop Diego in any way, or that is owned, leased or controlled by Bishop Diego, including files created, stored or found on Bishop Resources, Personal Resources or elsewhere, or files that have Personal Identifying Information

register to select, on a Device, an open unsecured WiFi account provided by Bishop Diego for Guests, consent to be bound by the Acceptable Use Policy, and agree to all its terms and provisions

Request for Access to Records a court order, search warrant, request for production of documents, subpoena, demand or request for Bishop Records, Software, or Personal Records or Software, issued by: i) a court of law; or served by: ii) a law-enforcement agency, party in a criminal proceeding, or police- or other government-investigation; iii) a party to a civil lawsuit where Bishop Diego is a named litigant; or iv) a third-party in a lawsuit where Bishop Diego is not a named litigant

Resource, IT Resource, Bishop Resource all Systems and any other technology systems that allow access, review, modification, transmitting, modification, and/or storage of electronic information, Records or executing of Software, referred to as a "Bishop Resource" if owned, leased, controlled or administered by Bishop Diego; regardless of whether the Resource is owned by an external service provider

review/reviewing to access a Record or Software and learn or ascertain its contents or purpose, including, opening, retrieving, reading, analyzing, monitoring, examining or scanning it, whether done by an Authorized Administrator or automatically by a filter or content-control software

Software a computer program, usually one of two types: system software/utilities (needed to operate or maintain the computer), and application programs (which enable the user to perform a useful task using the computer) often called an "application" or "app"

store, storing the saving, backing up, preserving or safeguarding of Records; computer data storage is a technology system consisting of computer components and recording media that are used to retain digital data, a core function and fundamental component of computers

[3] The definition of "Record" is intended to be much broader than the definition of "record," a narrower term relating to a collection of related data and information items found in a database.

system an organized collection of components, e.g., Devices, Media and Software, that have been optimized to work together as a functional whole

System, Bishop System refers to one of many electronic communication systems in use by the Bishop Diego Community and Guests that vary by media and technology; such systems may use the Internet/World-Wide Web, intranets, networks, and various combinations of equipment/hardware, e.g., Devices, Media, and also Software and Records; such systems include, but are not limited to:

1. e-mail/web-mail,
2. forums/posting content to web-sites (Facebook, LinkedIn, Twitter)\
3. text and instant messaging/private chat-rooms,
4. IRC (internet relay chat-room),
5. IP Telephony and VoIP (voice-over-internet protocol),
6. video-conferencing/video-chat systems,
7. services, including cloud-based services,
8. A/V multimedia systems,
9. networks,
10. data storage systems,
11. phone calls,
12. voice mail,
13. paging, e-mail and voice-mail through SMS,
14. facsimile machines, and
15. any other electronic communications system that may exist, be in use, or is created in the future and is used by Faculty, staff and/or Students.

technology in general, a complex human enterprise that integrates numerous resources (such a skills, scientific knowledge, technical expertise, experience and imagination) into an ongoing enterprise, often centered around a specific technological development (e.g., cellular phone technology, computer processor technology, smart-phone technology, etc.), with multiple stakeholders including, among others, officers, administrators, staff, and users

transmit any action that may be taken to move or send the original or a copy of a Record or Software including retrieving, receiving, copying, sending, distributing, forwarding, posting, turning-over, disclosing, downloading (User copies to his/her Resource from another source) and uploading (User copies from his/her Resource to another source)

User any person, such as a member of the Bishop Diego Community or Guest, who:

1. has agreed to all of the terms and provisions of the AUP and consented to be bound by it, has been assigned an Account and is thus authorized to use Bishop Resources, or

2. has registered to use the Guest Wireless Network (1. and 2. are "**Authorized Users**," i.e., authorized to use Bishop Resources), or

3. has not been authorized to use Bishop Resources (an "**Unauthorized User**") but who nonetheless hacks or attempts to hack Bishop Resources (Systems, Devices or Media) or Records, or the Personal Resources or Records of third parties

User Consent express consent provided by a User (or by a parent or guardian if the User is a minor) authorizing Bishop Diego to access, use, and disclose Records, Software or other Electronic Information to a third party pursuant to a Request for Access to Records

Wide Open Access Rights are elevated or unlimited access rights (such as the right to access the contents of all User Records but only for legitimate administrative interests) given pursuant to an authorization specified in a job description), that accompany the duty/responsibility to: protect individual passwords, maintain the safety or security of the Bishop Diego Community, or act to ensure the uninterrupted operation of Bishop Resources—while avoiding direct or indirect contact with a User's Records and information and electronic communications content whenever possible

I. ELECTRONIC COMMUNICATIONS POLICY

INTRODUCTION:

The Electronic Communications Policy requires that all Users of Bishop Resources use electronic communications in a responsible manner, consistent with applicable law, the school's Catholic mission, and adhere to the morals and values of the Catholic Church; all Users are expected to respect others and to follow the Electronic Communications Policy, and the standards and policies of Bishop Diego.

Users Covered by the Electronics Communications Policy

All Users are required to follow the Electronic Communications Policy, including all members of the Bishop Diego Community—students, Faculty, and staff—and any Guest who uses Bishop Resources, or Personal Resources in a manner where Bishop Diego, the campus, or school activities may be implicated in their use regardless of location, i.e., whether on-campus, home, or elsewhere.

Violation of Federal and State law, Regulations, Codes of Conduct Prohibited

Users of Bishop Resources and Personal Resources shall not violate any federal, state, or local law, regulation, code of conduct, code of ethics, safe environment or educational rule.

Consequences of Violation of the AUP/Electronic Communications Policy

Violations of this policy, including breaches of confidentiality or security, may result in the restricting of access to Bishop Resources, suspension or termination of electronic communication privileges, confiscation of Bishop Diego Devices or Media, or of Personal Resources on which Bishop Records are found and, depending on the gravity of the violation, disciplinary action up to and including removal from school activities, discharge from employment, removal from parish activities, the reporting of the violation to law enforcement, being asked to leave and/or escorted off-campus, and/or other appropriate disciplinary action.

Access to and use of Bishop Diego's Bishop Resources may be wholly or partially rescinded by Bishop Diego without prior notice and without the consent of the User when necessary in the judgment of the Head of School or Authorized Administrator.

A student found to have violated policies in the AUP may also have violated Bishop Diego's "Core Values that Guide Student Norms of Conduct." (High School Handbook at _) An employee found to have violated the AUP may also have violated other Bishop Diego employment policies. All are subject to appropriate disciplinary action for violation of the AUP.

BISHOP DIEGO'S RELATIONSHIP TO IT RESOURCES AND RECORDS

Ownership of Bishop Resources; Nature of Use

Bishop Diego owns, controls and administers substantial IT Resources (called "Bishop Resources") in its buildings and classrooms, including Portable Devices and Media that are taken off-campus from time to time. Bishop Resources are provided to Users primarily to further the educational and Catholic Mission of the school. Use of Bishop Resources is provided to employees to facilitate educational, administrative and business matters. All Bishop Resources shall be used primarily to conduct school business, not personal matters. Employees should use only those Bishop Resources that they are authorized to use, and only in the manner and to the extent authorized.

Ownership of Records; Nature of Use

Bishop Diego owns and licenses extensive, commercially available Records and Software; Bishop Diego also owns any and all Records and Software that Users (such as students, Faculty and staff) and Guests create, access, modify, transmit or store on Bishop Resources and, potentially, on Personal Resources. For example, Bishop Diego owns all "apps" that its students, Faculty or staff create throughout the school year, including those that students design for iOS (mobile operating systems) for their classes.

All such Records and Software wherever found are related to the educational, administrative or business affairs of Bishop Diego; and to student activities, student life, and implicate Bishop Diego as an institution. All such Records and Software constitute the property of Bishop Diego. All Users are required to take reasonable steps to maintain the confidentiality of Bishop Records and Software. (See Access Procedures at _ and User Restrictions at _) Accordingly, all Records created, transmitted, used, or stored by employees on Bishop Resources are expected to relate to Bishop Diego educational, administrative and business matters. Incidental personal uses are permitted as provided in the Employee Electronic Communication Guidelines.

Accessing Bishop Records Without User Consent:

1. Reservation of Rights for Regular, Necessary Activities

Bishop Diego reserves the right to take the following actions (1.-5.),[4] without notice to or consent of the User, with respect to Bishop Records and Personal Records that are stored or modified on, or accessed or transmitted through, Bishop Resources, regardless that the User may intend that such Records be private.

1. Actions to Ensure Continued, Effective School Operations

Bishop Diego reserves the right to access, review, modify, transmit and store Records or other Electronic Information without User Consent in order to ensure continuous uninterrupted operations and school activities; and under circumstances where failure to do so would likely cause Bishop Diego to fail to meet mission-critical governance, administrative, and/or teaching obligations.

2. Maintenance, Inspection, Back-Up Activities

To ensure the proper functioning and operation of Bishop Resources in connection with daily, ordinary operations, and audits or investigations, such resources require ongoing maintenance and inspection to protect Records against security threats such as cyber attacks and malware; the backup and caching of Records to protect against the failure of Bishop Resources; the review and scanning of Records downloaded from the internet and from portable memory devices to protect against viruses; and the logging of activity, the monitoring of general use and usage patterns, and other such activities to provide ongoing maintenance. To perform this work, Bishop Diego IT personnel and approved vendors under contract may access, review,

[4] A***ll Users could have their Personal Records legitimately accessed by Bishop Diego without their consent***. Bishop Diego's IT Resources allow Administrators to access i) all Bishop Records and other information generated by User interaction with Bishop Resources, ii) Personal Records and Electronic Information created by Bishop Resources or Personal Resources, when stored or transmitted through Bishop Resources, and iii) Activity Data (User interaction with Bishop Resources generates Activity Data that can be attributed to individuals using Personal Resources).

Electronic Communications are enduring if not permanent: Even when a Record or Personal Record, such as an e-mail, has been deleted, it may still exist on a backup system, be restored, printed, or inadvertently forwarded to someone else without its creator's knowledge. Once placed upon Bishop Resources, the contents of Records, Personal Records and Software cannot be considered private or confidential to the User.

modify, store and transmit Bishop Records and Personal Records without User Consent. Bishop Diego may also permit third-party service providers under contract the same rights vis-à-vis Bishop Records to in order to provide, maintain or improve services to Bishop Diego.

When possible such persons shall avoid accessing Records or other Electronic Information where access is not relevant to system maintenance and support; unavoidable examination of Records or other Electronic Information shall be limited to the minimum required to perform such duties.

3. Actions Necessary Prevent Access to Malicious Materials & Ensure Safety

Bishop Diego follows certain protective provisions of the Children's Internet Protection Act including the use of Internet filters, and implementing other measures to protect children from harmful online content. Bishop Diego continuously accesses, reviews, and scans all Bishop Records and Software, and Personal Records and Software, and other Electronic Information, that is found on: i) Bishop Diego Resources, and ii) Personal Resources, in order to protect the safety of individuals and to ensure that students do not have any access to harassing, obscene, pornographic, or threatening messages that are a violation of applicable law or Bishop Diego policies.

To ensure this protection, Bishop Diego, approved vendors and service-providers may take additional actions and, if necessary, will modify and safeguard for turnover to law enforcement Bishop Records and Personal Records that have been identified as containing malicious content, without notice or User Consent. Bishop Diego may demand turnover and confiscate Personal Resources if deemed necessary to further the purposes of this policy, in the discretion of the Head of School, Dean of Students, Director of Technology, Director of Technology or other Authorized Administrator.

4. Actions to Report Possible Violations of Law

If in the course of their duties Bishop Diego Faculty or staff inadvertently discover or reasonably suspect a violation of law or Bishop Diego policy, such personnel shall inform the Dean of Students and the Director of Technology, either of whom may investigate and preserve Bishop Records, Personal Records and other Electronic Communications and report the results of the investigation to the Head of School; the Head of School may in appropriate circumstances report possible violations to law enforcement and, if such a report is made, shall inform the Board of the same.

Bishop Diego co-operates with law enforcement and other authorized government officials without prior notice or User Consent. Bishop Diego reserves the right to disclose to law enforcement officials all Records accessed, modified, transmitted or stored on Bishop Resources or Personal Resources, and may provide such officials with copies of the same, as may be deemed appropriate in the discretion of the Head of School or an Authorized Administrator.

5. Actions Pursuant to Court Order/Subpoena (Request for Access to Records)

In general Bishop Diego complies with all lawful Court orders, demands of government agencies, and Requests for Access to Records issued in litigation that have not been quashed or vacated pursuant to Court order. All Requests for Access to Records arising out of law or legal process shall be referred immediately to the Head of School.

Under some circumstances, as a result of receipt of a Request for Access to Records (pursuant to a lawsuit, investigation, police or other governmental proceedings), Bishop Diego may be specifically required to provide Bishop Records, Personal Records, or other electronic information relating to a User ***without notice to or consent of the User***.

Notice

Unless law, court order or policy mandate confidentiality, delay in disclosure, or that no notice be provided, in the discretion of the Head of School Bishop Diego shall notify the affected User (or the User's parent or guardian if the User is a minor) at the earliest opportunity that is lawful of the action(s) taken and the reasons for the action(s) taken.

6. Procedure to Initiate Investigation to Access Bishop Records

Reservation of Rights

In addition, Bishop Diego personnel may learn of information indicating that there is reasonable suspicion for believing that a User may be violating the AUP, other Bishop Diego policies, or applicable law which, in order to preserve the integrity of the evidence, may warrant initiating an investigation that accesses Bishop Records, Personal Records, and other Electronic Information *without notice or User consent*. Bishop Diego reserves the right and discretion to determine whether to institute such an investigation. The Head of School, Dean of Students or other Authorized Administrator shall evaluate all the relevant circumstances including the

possible effect of access on Bishop Diego and its values as an institution in making the determination.

Who May Initiate an Investigation

Except for circumstances arising above under paragraphs 1-5 above:

A. if the person suspected is an **Authorized User** such as:

1. **Faculty member or staff**: the Head of School is authorized to approve an investigation with delayed notice and/or without User consent. The Head of School may delegate this authority to an Authorized Administrator; and may also designate other personnel to assist with such investigation. Whomever is authorized shall prepare a report regarding the results of the investigation.

2. **Student, Guest or member of the Bishop Diego Community**: the Director of Technology and Dean of Students are authorized to initiate an investigation without notice or User consent; if initiated by the Dean of Students, the Director of Technology or other IT personnel shall assist the Dean of Students in accessing and reviewing Bishop and Personal Records found on Bishop Resources or Personal Resources; whomever conducts the investigation shall prepare a report and inform the Head of School of the results of the investigation.

Authorization shall be limited to the least intrusive means needed to investigate the Records, but sufficient to comply with Bishop Diego's legal and policy obligations. Nothing herein is intended to limit Bishop Diego's duty to comply with applicable law.

B. if the person suspected is an **Unauthorized User**, the Dean of Students or Director of Technology may initiate an investigation without notice, User consent, consideration of privacy interests, nor consideration of limiting the investigation to the least intrusive means.

Notice

At the earliest opportunity that is lawful while preserving the integrity of the investigation, Bishop Diego shall notify the affected User(s) (or the User's parent or guardian if the User is a minor) of the action(s) taken, the reasons for the action(s), and the results of the investigation unless law or policy mandates confidentiality or delay in disclosure, in the sole discretion of the Head of School.

7. Record/Log

The Authorized Administrator who approves access to Records, whether pursuant to Court order or subpoena (¶ 5 above) or to an investigation (¶ 6 above), shall create a complete record of the authorization. The record shall include, where applicable:

a. a description of the Record(s) that are accessed, and the date, time it occurred,,
b. the justification for the access,
c. whether legal process was employed to compel the access,
d. whether the subpoena, request for production of documents, or court order required confidentiality or that delayed, or no notice be given (a "gag" order), and
e. whether/when the User was notified, and
f. whether/when User Consent was obtained

The record shall be submitted to, and/or kept by, the Head of School.

The Director of Technology shall be responsible for keeping a summary log of instances of access to Records without notice or User Consent, with the identity of the User redacted. This log shall be made available to the Board annually.

The Board has the right to request further information, to review a record, and/or to create an *ad-hoc* subcommittee to monitor developments relating to litigation or an investigation to report to the Board, as the circumstances warrant.

8. No Expectation of Personal Privacy

Each of the foregoing reserved rights and duties (1.-6.) are designed to protect Bishop Diego, its students, Faculty and staff, enhance the security and confidentiality of Records, and ensure compliance with federal and state law; their exercise and performance, however, necessitate that individual personal privacy may be invaded. The personal security of Bishop Records and of Personal Records cannot be guaranteed to any User. ***Users therefore have no reasonable expectation of personal privacy with respect to Bishop- or Personal Records created, transmitted to, or stored on Bishop Resources, or Personal Resources when they are related to Bishop Diego's educational mission, administration or business, or to student activities or student life, or implicate Bishop Diego in any way.***

Procedure for Disclosure of Records/Electronic Information to Third Parties

Even under circumstances where Bishop Diego may legitimately access Records without notice or User consent (1-6 above), it will not ***disclose*** such Records to third parties such as government officials or law enforcement without notice or User Consent unless Bishop Diego is required to:

1. **protect against bodily harm** to humans or animals or significant property loss or damage, and time is of the essence;

2. **report a crime** relating to or indicated by the Record or other Electronic Information;

3. **by law or legal process** See 5. above, procedure outlined at _, ¶ _ (Actions Pursuant to Subpoena or Court Order (Request for Access to Records))

Otherwise, Bishop Diego will make reasonable efforts to provide the User (or the User's parents or guardian if the User is a minor) with a Notice of Third Party Request and attempt to obtain User Consent. Where notice may be provided and Bishop Diego does not have evidence that a User has received a copy of a Request for Access to Records, the school will provide a copy of the document to the User. Sending a Notice of Third Party Request with a copy of the Request for Access to Records via e-mail shall constitute sufficient reasonable efforts, although other communication methods may also be employed (mail, facsimile, phone).

Bishop Diego will attempt to provide timely Notice of a Third Party Request sufficient to enable the User to object to the disclosure in Court.

If the User's Bishop Records (e.g., employment Records requested in personal injury litigation) or Personal Records are at issue, the User is responsible for moving to quash the Request for Access to Records or taking other appropriate legal action. Users in this situation should seek legal counsel for assistance.

Bishop Diego's policy is to comply with legal and governmental processes in the absence of the User successfully obtaining a Court order sustaining an objection to the Request for Access to Records (i.e., a Court order quashing a subpoena or order having similar affect).

Record Retention in Anticipation of Legal/Governmental Proceeding

It is the responsibility of all Faculty and staff to preserve all relevant Bishop Records and Personal Records (collectively, “Records”), including messages and emails, whenever they have actual knowledge of matters in which a civil or criminal court action will likely be commenced.

When considering what Bishop Records and Personal Records to preserve and store, Faculty and staff should recognize that the duty to preserve and produce evidence will apply to the entire universe of Bishop Diego Resources and Personal Resources on which such Records may exist, including computers, notebook or other portable computers, PDA's, smart phones and removable storage devices such as flash drives or writeable optical disks, and Cloud Based Storage. Employees shall follow all Bishop Diego policies and directives regarding the preservation of Records.

Discretion To Inform Where User Has Minimal or No Connection To Bishop Diego

Situations may arise where the Faculty or staff learns that a person who is not an authorized User and who is not using Bishop Resources, is sending electronic communications or using Personal Resources off-campus in a manner that may be improper, immoral or possibly illegal; and the circumstances are too unconnected to Bishop Diego and the Bishop Diego Community for it to be appropriate to initiate an investigation or otherwise be a concern of the Administration. As to minors, parents in these situations remain responsible for the supervision of their son or daughter. The Head of School, however, shall have the discretion to contact a parent (in the case of a minor), other responsible party, or law-enforcement to alert them to the matter. The Head of School may delegate such task to an Authorized Administrator.

ACCESSING BISHOP RESOURCES – PROCEDURE

Authorization to Create an Account; Creating Accounts, User IDs and Passwords

Bishop Diego provides access to Bishop Resources based upon a demonstrated educational, administrative or business need by creating an Account for each User. Limiting access to Bishop Resources helps prevent unauthorized access to such resources and to Bishop Records. The following policies are designed to protect the confidentiality of Bishop Records, not to provide or assure Users of personal privacy.

Access to Bishop Diego Resources, Records and Software is conditioned upon an Authorized Administrator, designated by the Head of School, certifying the following in writing to the Director of Technology:

1. an authorized relationship with Bishop Diego: for example, students, Faculty, staff, IT service providers, and in limited circumstances vendors and contractors; certification of a class of individuals, e.g., all enrolled students, all teachers under contract, all IT employees, etc., is permitted,

2. an identified Legitimate School Reason; the function should be listed with specificity,

3. approval to access specific, identified information domains, directories, folders, etc., and

4. authorization to create an Account and issue a unique User ID and password for each individual and/or each member of a certified class (see item 1. above) to be granted access to Bishop Resources.

The creation of an Account for a person or entity is also subject to the person or entity providing the following to an Authorized Administrator:

5. an agreement and consent in writing to the terms and provisions of the AUP, all applicable Bishop Diego policies, and applicable law (i.e., a "Bishop Resource Access Agreement"),

6. as soon as may practicably be implemented, the person or entity has executed a separate release of claims, agreement not to sue, and hold-harmless agreement (referred to as the "Agreement to Assume Risks of Participation in Bishop Diego Electronic Communications Systems, Waiver, Release of Claims/Liability, Hold Harmless, and Indemnification").

Once the foregoing conditions for creation of an Account have been satisfied, every Account created shall include the following:

1. User ID,
2. initial password (to be changed by the user),
3. any information necessary to keep track of the User, and
4. designation of the domain, computers, file systems, directories, folders, and Records that each User is allowed to access.

Notice of Password Requirements: A User's password shall not be stored on Bishop Resources. Users shall be initially notified of password requirements such as composition, the time period that initial and user-modified passwords remain valid, and how to recover lost passwords.

Guest Wireless Network: Bishop Diego does not require an Account and User ID be established for Guests who seek temporary wireless access to the internet. Such Guests may register to use the Guest Wireless Network. Such access is temporary; and the Network is an open, unsecured WiFi account, that does not allow access to any other Bishop Resource. Consent to the AUP, before connecting a Personal Device to the Guest Wireless Network, is mandatory.

In the absence of being provided with an Account or registering for the Guest Wireless Network, the use of Bishop Resources is prohibited. Members of the Bishop Diego Community and Guests shall be advised not to attempt access to Bishop Systems without authorization by notice posted in appropriate written materials. (Unauthorized persons who, nonetheless, use or attempt to use Bishop Resources without being authorized are considered "Users" of Bishop Resources; and subject to all policies of the AUP and potential penalties and sanctions for violation of such policies).

Account Security: Bishop Diego requires that Accounts, User IDs and passwords be used only by the owner of the Account. Accounts, User IDs, and passwords are non-transferable; Users must keep their Account, account information, User ID, and password confidential.

Authentication: All Bishop Resources that create, store, transmit, or publish information or data (e.g., a website) must have authentication (the ability to verify the identity of the user) and authorization systems installed at the earliest time practical, as school budgeting permits, to prevent unauthorized use, access, and modification of Bishop Records and Software.

Accounts shall be recorded and updated in a centralized user directory or authentication system (accounts for technology systems not included in such directory or system must be on-record with the Director of Technology).

Unauthorized Use of an Account, User ID or Password

Users shall not:

1. agree to share an Account, account information, User ID, password, or online identity,

2. give or enable unauthorized individuals (employees, students or volunteers) access to Bishop Resources or Records nor jeopardize their security by allowing unauthorized use or disclosure of Accounts, User IDs, or passwords, and

3. seek or gain unauthorized use of or access to, or trespass on, someone else's Account, User ID or password; or damage, alter, disrupt the information in the Account.

Anyone suspecting that their Account has been compromised should contact the Director of Technology, at 805 967-1266; and dyokubaitis@bishopdiego.org.

PERSONAL RESOURCE USE—RESPONSIBILITIES

Personal Resource Use for Educational and Other Purposes

Bishop Diego does not require students, Faculty or staff to use their Personal Resources for Bishop Diego educational, administrative or business purposes. An Authorized Administrator or Teacher, however, may authorize such use; and may authorize Faculty or staff, or students, respectively, to connect or attach their Personal Resources to Bishop Resources. When authorized, Users may bring Personal Resources on-campus and use such Resources. ***The Authorized Administrator or Teacher, however, must inspect approve the Personal Resources before attaching it to Bishop Resources.*** Any Personal Resource used for Bishop Diego educational, administrative or business activities, or student activities, student life, or implicates Bishop Diego in any way, is subject to the AUP.

Responsibility for Personal Resources

1. All Users are solely responsible for their Personal Resources and shall permanently label devices with identifying information.

2. Users shall keep their Personal Resources secure at all times and not loan them to others, unless required to do so for an educational assignment or, in the case of teachers, by their job description or as approved by an Authorized Administrator.

3. Bishop Diego assumes no financial responsibility for Personal Resources if they are lost, loaned, damaged, or stolen.

If information is obtained that a User is utilizing a Personal Resource or their functions in a manner that may violate Bishop Diego's policies, the AUP or applicable law, the User may be required to turnover the Personal Resource for inspection and possible confiscation:

1. If the User is a student, the turnover process is governed by the Parent-Student Handbook, "Protocols Regarding Substance Abuse, Searches & Interquest" at _. The student will be subject to consequences in accordance with the Bishop Diego's disciplinary policies and procedures.

2. If the User is a teacher, administrator or staff, this process is governed by _, and such Users will be subject to consequences in accordance with the Bishop Diego Employee Handbook. The Head of School shall be authorized to determine whether to demand turnover of Personal Resources where Faculty or staff is involved.

Personal Resources must conform to all Bishop Diego requirements regarding the types of Devices and Media that are authorized to connect to Bishop Resources. The Personal Resource must also comply with any additional requirements including security controls for encryption, patching and backup, specific to the particular function for which it is used.

USER RESPONSIBILITIES AND RESTRICTIONS FOR SECURITY/CONFIDENTIALITY OF RECORDS:

As the following sections indicate, there are many ways that communications in Records can be malicious, harmful, disruptive, burdensome or illegal. Given the setting of a High School with a large population of underage minors, Bishop Diego reserves the right to, among other things, modify, even to the extent of deleting without notice (and potentially safeguarding for turnover to law enforcement), any Record found on Bishop Resources deemed to be harmful, in

circumstances where the Head of School or Authorized Administrator determines that it is necessary to do so. (See Employee Electronic Communication Guidelines at _)

Scanning Records and Software for Viruses/Unauthorized Records and Software

All Records and Software downloaded from the Internet or uploaded from Personal Devices or Media onto Bishop Resources, and all computer disks received from outside sources, must be scanned with updated/current virus detection software. Contact the Director of Technology for guidance. Immediately report any viruses, malware, or other system breaches to the Director of Technology and the Head of School.

Users shall not utilize any Bishop Resource or Personal Resource for designing, developing, distributing, running/executing, or storing any Software unless explicitly required by their job description or approved by an Authorized Administrator.

Content Filters

Minors may only access the Internet from Bishop Resources that use filters to eliminate prohibited content that are updated and functioning. All obscene materials, child pornography, pornography, or materials that are otherwise harmful to minors or in violation of this Electronic Communications Policy must be blocked. Before allowing minors to access the Internet, a teacher, parent, responsible person or other User must ensure that content filters are "ON" and that active filtering of prohibited materials is enabled. Content filters for minors shall not be disabled or turned "Off" without obtaining prior authorization from the Director of Technology.

Protection of Confidential Information/Misuse of Records and Software

Users shall abide by the following Record handling and transmission policies. Users shall not:

1. disrupt, modify without authorization or for purposes other than a Legitimate School Reason, interfere with access to or use of, or engage in other activities that damage, vandalize or otherwise compromise the integrity of, Bishop Records or Software,

2. share, give away, or disclose Records or Software in a way that violates applicable policy, procedure, or other relevant regulations or laws,

3. trespass on another User's work-station when they are away from it; make changes to their work in memory, folders, Bishop Records, Personal Records or Software; alter, modify, delete, obtain copies of Records or Software, Personal Records, or any other digital content owned by another User without the permission of the User, their supervisor or, in the case of students, a Teacher or Authorized Administrator,

4. install, download or introduce any unauthorized Software, virus, malware, tracking devices, or recording devices onto Bishop Resources, or run or execute such Software, without permission from the Director of Technology or Authorized Administrator,

5. use Bishop Records for personal use or benefit,

6. attempt to breach Bishop Resource security,

7. alter, without authorization, a startup screen or desktop, or install applications that will subvert these functions,

8. inadequately or negligently protect Records, Software or other information; or ignore the explicit requirements of owners for the proper management, use, and protection Records, Software or other information,

9. forward a Record, such as an e-mail that was sent privately, without permission of the person who sent the e-mail,

10. alter and forward a Record, e.g., an e-mail, in a manner that misrepresents the original message or message chain,

11. give away information or send bulk unsolicited email without appropriate authorization,

12. tamper with any Bishop Resource or Personal Resource of another User in a way that affects Bishop Records or Personal Records, or

13. access, intentionally seek or provide information to which the individual has no legitimate right.

Unauthorized Transfer Sensitive, Proprietary, or Personal Identifying Information

All Bishop Records with Personal Identifying Information, or that contain proprietary or sensitive information, are confidential. Shall follow the following procedures when handling such Records:

1. Users shall not access, modify, review, store or transmit such Records, without permission from an Authorized Administrator or Teacher (in the case of information about a minor), unless the User's duties or responsibilities assigned to them or set forth in their job description authorizes them to dispose of Records in the manner described above. (See Employee Electronic Communication Guidelines).

2. When an Authorized Administrator or Teacher authorizes a User to access such Records, Users shall not:

    a) use or dispose of the Records other than in the manner authorized,

    b) show such Records to an unauthorized person,

    c) transmit such Records to an unauthorized recipient, or

    d) allow anyone to access such Records:

        i. who does not have a Legitimate School Reason for doing so, or

        ii. allow anyone to access such Records if they do not require knowledge of the data or information in such Records.

Facsimile If authorized to such confidential information by facsimile, Users shall send such Records only after confirming that the receiving fax machine is located in a secure area accessed only by those with a legitimate need to see the information.

Appropriate Handling of E-mails

Users shall follow these policies regarding the handling of Records containing messages, such as e-mails, that have any educational, administrative or business purpose, or are related to student activities, student life, or implicate Bishop Diego in any way:

1. Users shall use Bishop Diego's e-mail service exclusively to send and receive all such Records.

Users shall not:

2. use Personal Resources including Devices to send e-mails for work purposes,

3. open or download e-mail attachments from unknown senders, and

4. e-mail confidential Bishop Records to non-Bishop Diego e-mail addresses unless the file is appropriately encrypted pursuant to procedures of the Technology Department regarding transmission of such Confidential Records.

(To obtain assistance regarding procedures regarding encryption technology, contact the Director of Technology).

5. send e-mails or other Electronic Communications to groups such as "All Employees," "All Parents/Guardians," and the like, on the intranet, network or World Wide Web, unless approved by an Authorized Administrator before the message is sent.

Administrators shall ensure that students do not have such sending options with respect to any Account assigned to them, or Bishop Resource that they may use.

Defamatory, Offensive, Harassing or Disruptive Communications

The transmitting of Records including messages, e-mails, texts, pictures and images which a reasonable person, according to the teachings of the Roman Catholic Church, would consider to be defamatory, harassing, disruptive, derogatory, bullying, or so offensive as to amount to bullying, is prohibited.

Prohibited messages and images include, but are not limited to, sexual comments, racial or ethnic slurs, or other comments or images that would offend a reasonable person on the basis of race, creed, gender, national origin, sexual orientation, age, political beliefs, mental or physical disability, or veteran status.

Additional actions that Users are prohibited from taking include, but are not limited to, the following:

1. engaging in improper fraternizing or socializing between adults and minors,

2. engaging in cyber bullying, sexting, shaming, or other abusive online behavior

3. minors agreeing to meet someone they have met on-line without their parents' approval or without the presence of a parent at any meeting,

4. knowingly access, view, download, save, create and post, send, or distribute fraudulent, harassing, indecent, obscene (i.e., pornographic), brutally violent, threatening, or other messages or materials, including from messages created using Personal Resources sent from home to other people through an on-line forum,

5. contributing to the creation of a hostile educational, academic or work environment,

6. the recording of any telephone or other conversation without the express permission of the other participant to the conversation, except where allowed by law, and

7. the posting of chain letters or engaging in "spamming" (sending annoying, unnecessary or unsolicited commercial messages).

Forums

Bishop Diego Faculty, clubs, parent volunteer organizations, students and other groups may host forums. Student forums relating to an academic department or to an extra-curricular club must be sponsored, hosted, and monitored by a Teacher or Administrator.

Additional Conditions of Use for Forums

Teachers and Authorized Administrators who host or supervise an online forum for students may define additional policies and conditions/requirements for joining, continued participation, and the use of information resources under their control or supervision (collectively, "Additional Conditions of Use"). These conditions/requirements must be consistent with the AUP and school policies, but may provide additional detail or guideline restrictions. Where such conditions/requirements are established, the host Teacher or Administrator is responsible for publicizing and enforcing the Additional Conditions of Use.

As a condition to establishing a forum, forum homepages where they exist and each individual forum page, shall contain a header that notes whether additional terms of use have been

posted by the host. If so, the header should state: "Subject to Additional Terms of Use." Users are required to agree to the Additional Terms of Use before being permitted to participate in the forum. Users shall comply with all Additional Conditions of Use and any conditions set forth for participating. Users must in all circumstances respect the purposes of the forum.

Unauthorized Use of Bishop Diego's Name on Social Media

Users shall not create any internet presence (e.g. on a social media page such as Twitter, Snapchat, Instagram, or Facebook) that uses all or any part of the name Bishop Garcia Diego High School, unless the presence is owned or controlled by Bishop Diego and approved by an Authorized Administrator.

Unauthorized Use of Bishop Diego Images, Logos

Users shall not use the name, logo, identifying photograph, mission statement, or other unique identifying information of Bishop Diego on a non-Bishop Diego website, forum or other online service in such a manner that readers/viewers would be lead to believe that the site was an official site or media controlled by Bishop Diego.

Trademarks

Users shall not upload, download, view, save, copy, transmit or otherwise distribute to third persons, trade secrets, trademarked, patented, or other confidential, private, or proprietary information, or other materials to which the User does not have access rights.

Political Use

Bishop Resources shall not be used for political activities, partisan or otherwise, with the following exception: Personal Resources connected to Bishop Diego's Guest Wireless Network (i.e., the Guest WiFi account for wireless internet access), and not WiFi accounts designated for students, teacher or administrators, may be used for non-partisan political activities only when in compliance with applicable federal and state laws, applicable Bishop Diego policies, outside regular school/business hours.

Excessive or Burdensome Use of Bishop Resources

Users should respect the finite capacity of Bishop Resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. The reasonableness of the particular use will be judged in the context of all relevant uses and resources.

Commercial Use

Bishop Resources shall not be used for commercial purposes, including advertisements, solicitations, promotions or other commercial messages, except as permitted under Bishop Diego policy. Any such permitted commercial use should be properly related to Bishop Diego activities (e.g., Cardinal Club advertising). The Head of School or other Authorized Administrator will determine permitted commercial uses.

Use of Bishop Resources for Personal Matters

Bishop Resources shall not be used for personal activities unrelated to appropriate Bishop Diego functions and activities during class, except in an incidental manner. Employees and students may access the internet outside regular school/business hours or during breaks.

Student Use of Personal Resources for Personal Matters

Students shall not use their Personal Devices or Media, or access personal e-mail, file storage, Cloud Based storage, file-sharing services, or other communications and collaboration services (personal Gmail, Yahoo! or Hotmail accounts), for personal matters except i) during breaks, or ii) in urgent or emergency circumstances if approved by a Teacher or Authorized Administrator. Bringing any Devices or Media on campus during the school day makes such Resource subject to the AUP.

Reporting or Security Incidents/AUP Violations

Users must report suspected security incidents/violations of the AUP to the Dean of Students and Director of Technology; and will immediately report concerns with system security, or suspected unlawful or improper system activities during normal business hours.

Examples of suspected security incidents include:

1. attempts (either failed or successful) to gain unauthorized access to Bishop Resources or its data,

2. theft, destruction, or other loss of any Resource, Device or Media whether or not such item is owned by Bishop Diego

3. unwanted disruption or denial of service,

4. the unauthorized use of a System for the processing or storage of data, and

5. changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Inspecting and monitoring information and information resources may be required for the purposes of enforcing this policy, conducting investigations or audits, ensuring the safety of an individual, complying with law, or ensuring proper operation of information resources.

Cooperation Expected

Users are expected to cooperate with any investigation of security incidents or potential violations of the AUP or other Bishop Diego policies. Lack of candor or failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.

RESTRICTIONS THAT PROTECT BISHOP RESOURCES (HARDWARE AND EQUIPMENT)

Additional Requirements for Off-Campus Computing and Communications

Portable Devices, whether owned by Bishop Diego or a Personal Resource, pose an increased security risk, and risk of theft, due to their portability. Users must take extra care to secure Devices and electronic communications when traveling.

Students, Faculty and staff who leave campus with portable Bishop Resources, such as Multimedia Equipment, portable Bishop Devices and Media and, potentially, portable Personal Resources, must take additional steps to protect any Bishop Records found on such equipment, and to protect the security of Records/electronic communications. Such Users shall:

1. encrypt data storage on Bishop Devices and Portable Device, protected by a password,

2. do not access, store or transmit proprietary, sensitive or Confidential Records via such devices without prior approval of an Authorized Administrator,

3. use an encrypted communication channel for these activities.

Before leaving, contact the Technology Department in order to implement any required security measures for off-campus computing, and for information and assistance with encrypting Devices and communications.

Abuse of Bishop Resources/Computing Privileges

1. **Security Systems:** Users must not disable, defeat, render inoperative or bypass (via proxy servers or other means) any Bishop Resource security systems, firewalls, or content filters, or similar protections on the Personal Resources of other Users.

2. **Bishop Resources/Networks:** Users of Bishop Resources shall not access, alter, manipulate or modify Bishop Resources—Systems, networks, hardware, equipment, Software—or resources used to operate other sites, or intentionally enable others to do so, without proper authorization, *regardless of whether the IT resource is owned by Bishop Diego*. For example, abuse of an IT resource, device, or network to which Bishop Diego belongs, or the computers at other sites connected to those networks, will be treated as an abuse of Bishop Diego computing privileges. All Users are expected to protect Bishop Resources and physical hardware and equipment from unauthorized use. Faculty and staff shall monitor, control and safeguard local physical access and remote access.

3. **Devices and Media** Users shall access Bishop Resources only using Bishop Diego provided Bishop Devices or Media, or on specifically approved Personal Devices or Media.

Tracking of Bishop Resources (Systems, Devices, Media)

To ensure the responsible use, security and maintenance of Bishop Resources, the Director of Technology and IT personnel, assisted by Faculty and staff, shall whenever possible keep an up-to-date log identifying and tracking the use of such Resources, particularly when individual items are assigned to individual Users for authorized school activities. Such log shall include:

1. a brief description of the Resource (e.g., Device, Media), along with any unique identifying information,

2. purpose of use,
3. name of User/responsible party to whom the Resource is assigned,
4. date/time Resource issued,
5. date/time Resource returned, and
6. description of any change to the Resource arising out of the use (e.g., apparent damage or change in functionality).

For student activities in the classroom, the Director of Technology/Faculty may indicate that a class of Users has been assigned similar Devices (e.g., all students/Intro. to Multimedia, Sony mini-cameras, etc.).

Reimbursement for Lost or Damaged Bishop Resources, Records or Software

Negligence The Head of School shall have the discretion to request reimbursement from a User (e.g., students, Faculty or staff) for loss, breakage, or damage of Bishop Resources, Records or Software if caused by the User's negligence.

The Head of School shall have discretion to require that a Department (e.g., Athletic Department or the English Department) be charged for reimbursement of the Technology Department for negligent losses, breakage or damage to Bishop Resources, Records or Software.

Willful Misconduct Bishop Diego shall seek reimbursement from a User (e.g., students, Faculty or staff) for loss, breakage, or damage of Bishop Resources, Records or Software if caused by the User's *willful, malicious or dishonest acts (e.g., theft) or gross recklessness/negligence.*

Gross recklessness/negligence is an extreme departure from the ordinary standard of due care, for example: i) the entire failure to exercise care, or ii) the exercise of a degree of care so slight as to justify the belief that there was indifference to the interests of Bishop Diego and its property and, in the case of students, to the instructions of the adult supervisor. The want of care raises a presumption of conscious indifference to consequences.

Withholding from Wages Bishop Diego may withhold money from an employee's wages only when authorized by a wage assignment evidenced by a separate, notarized document signed by the employee and specifically identifying the transaction to which it relates; if the employee is married, the assignment must be accompanied by the signed consent of the employee's spouse; such assignment is limited to no more than 50 percent of the employee's salary and is revocable at any time.

Withholding from Final Paycheck Bishop Diego may deduct from a final paycheck the cost of tools or equipment not returned by a terminated employee within a reasonable time, if permitted by law or:

1. the employee gives Bishop Diego prior written authorization to do so, and

2. if the loss was caused by the employee's willful, malicious or dishonest acts or gross recklessness/negligence.

Sufficient written authorization includes any agreement by which Faculty or staff agrees to such a deduction including i) the employment agreement executed at the start of employment, or ii) an agreement signed by the employee when the policy related to deductions is adopted. For staff, the deduction shall be limited so as not to bring the employee's hourly rate below the minimum wage.

Other Remedies As determined by the Head of School, Bishop Diego may take other affirmative steps to discipline students and limit its losses from employee negligence or willful misconduct relating to losses, breakage or damage sustained to Bishop Resources, Records or Software:

1. Students Bishop Diego reserves the right to institute disciplinary proceedings against a student-User as outlined in the Bishop Garcia Diego Parent-Student Handbook 2018-19 (Grounds for Disciplinary Action at _).

2. Employees

a. Discipline If an employee causes damage or loss because of poor performance, the employee is subject to discipline in the same manner as employees with other performance issues.

b. Termination In the absence of a controlling employment contract, employees may generally be terminated at will. Bishop Diego reserves the right to impose discipline, up to and including termination, in any situation deemed appropriate by the Head of School. Willful or intentional misuse of Bishop Diego Resources, Records or Software resulting in significant loss may be grounds for immediate termination.

c. Civil Suit Bishop Diego reserves the right to file a civil suit or file a claim in small claims court to seek reimbursement for losses or damage to Bishop Diego Resources, Records or Software.

Unlicensed Radio Transmission Prohibited

Users are prohibited from using Bishop Resources to transmit any radio frequency signal that is not permitted and/or licensed by the Federal Communication Commission ("FCC") or that would violate FCC rules or policies.

ACCESS TO RECORDS UPON DEPARTURE FROM BISHOP DIEGO

Access to Email/Records

Bishop Diego maintains procedures for disposition of the email accounts and other electronic communications and files of Users, such as students and employees, who are leaving the Bishop Diego Community. Email account access, retention, forwarding, and automatic notification are configured by a Bishop Diego email administrator according to these procedures. Bishop Diego may in its discretion approve exceptions to the procedures. The process for employees to obtain access to their email or other Records after their separation from Bishop Diego is detailed in the Employee Electronic Communication Guidelines.

Record Destruction

See Table 1 for the retention period for Student-related Academic Records (AUP at _).

When records are no longer required to be retained and are no longer in active use, they should be destroyed or discarded. Non-confidential Bishop Records and, potentially, Personal Records found on Bishop Resources, may be deleted with simple file or email delete commands.

Confidential Records and Records with Personal Identifying Information that are stored on Bishop Resources may be disposed of in this manner. Confidential Records that have been stored on departmental file servers, stand-alone desktop computers, or on Bishop Media must be securely destroyed. This is typically done by overwriting the Record or by physically destroying the Media on which the record is stored. Contact the Technology Department or IT personnel for additional information on secure disposal methods for electronic data.

ADDITIONAL POLICIES APPLYING TO BISHOP DIEGO FACULTY AND STAFF

Training

Every staff and faculty member is responsible for completing any training offered by Bishop Diego for information and security practices.

All Personnel Are Responsible for Security and Protecting Bishop Resources

All members of the Bishop Diego Community, in particular the Faculty, are responsible for adhering to Bishop Diego security requirements, including but not limited to the following:

1. maintain up-to-date anti-virus software and system patches on all Bishop Resources including Bishop Devices; when prompted to update such software or patches do so as soon as possible,

2. store confidential Bishop Records, where possible, on appropriately encrypted medium; contact the Director of Technology to determine whether it's necessary for encryption technology installed on departmental computers.

Employee Obligations Regarding Accounts of Others

All employees must respect the privacy of Accounts and confidentiality of Records of other Users ***regardless of whether the Account or Record is securely protected***. This policy prohibits Bishop Diego employees and their agents from accessing Records and other Electronic Information except in accordance with this policy. Bishop Diego employees shall take necessary precautions to protect the confidentiality of Records and Personal Records encountered either in the performance of their duties or otherwise. Employees of Bishop Resources shall not disclose information about current or former students or employees to others. Such disclosure violates Bishop Diego policies, and laws protecting the confidentiality of such information.

Employee Use of Personal Resources for Personal Matters

Faculty and staff shall not use their Personal Devices or Media, or access personal e-mail, file storage, Cloud Based Storage, file-sharing services, or other communications and collaboration services (personal Gmail, Yahoo! or Hotmail accounts), for personal matters except during breaks, after school, or in emergency situations. Bringing any Personal Device or Media on campus during the school day makes such Device or Media subject to the AUP.

DISPOSAL OF OBSOLETE EQUIPMENT

When Bishop Resources, including Devices and Media, are ready for disposal, handling such equipment must follow certain procedures; such equipment not only contains hazardous Media but it may also contain confidential Records. To dispose of such items the User must contact the Technology Department at tel. (805) 967-1266 x 226 to arrange for the Bishop Resource

disposal. The Technology Department will recover any usable hardware/equipment and permanently delete any Records stored in preparation for disposal or storage, as appropriate.

GENERAL OVERSIGHT

Oversight of Bishop Resources and the AUP

Responsibility for, management, and operation of Bishop Resources is delegated to the Director of Technology. The Director of Technology, the Head of School or the Board may authorize access to Bishop Resources and Bishop Records for protection, maintenance, and management. Bishop Diego IT personnel, authorized employees, and authorized third-party vendors and service providers under contract, may access, review and maintain Bishop Resources, Bishop Records, Electronic Information, and Activity Data. Such persons shall avoid when possible accessing Records or other Electronic Information when not relevant to system maintenance and support; unavoidable examination of Records or other Electronic Information shall be limited to the minimum required to perform such duties.

This exception does not exempt any personnel from the obligation to protect Confidential Records and the prohibitions on unauthorized access and transfer of "Personal Identifying Information." (See Protection of Confidential Information/Misuse of Records and Software at _; Unauthorized Transfer Sensitive, Proprietary, or Personal Identifying Information, at _)

The Director of Technology will be responsible for compliance with all Bishop Diego policies relating to the AUP; and will be responsible for referring potential violations of the AUP to the Head of School. The Head of School may also designate a "system administrator" to manage and operate Bishop Resources, but responsibility for Bishop Resources and compliance with the AUP remains with the Director of Technology. The Director of Technology shall:

1. take all appropriate actions to protect the security of information and information resources,

2. take precautions against theft of or damage to information resources,

3. faithfully execute all licensing agreements applicable to information resources,

4. communicate the AUP, and other applicable information use, security and privacy policies and procedures to Users,

5. ensure that all critical Records, Software and other Electronic Information, whether related to Bishop Diego matters or personal to Users, is periodically backed-up onto storage in a safe place that is available for recovery in case of a loss of the original information; the Director of Technology shall formulate recommendations for Faculty regarding individual back-up procedures, if any,

6. ensure that contracts with third-party vendors, which will provide access to personally identifiable Bishop Records or Personal Records, shall include references to the AUP, to applicable privacy laws that protect Bishop Records, including Electronic Information and databases, and language that limits the third-party vendor from using or disclosing the Bishop Record or Personal Record, for any purpose other than to perform the services provided under the Agreement, or as required by law.

Wide open access rights

Persons who have Wide Open Access Rights (elevated or unlimited access rights), such as the Head of School, designated Authorized Administrator or IT service provider, in order to address a computer usage or repair issue, have special responsibilities. Such responsibilities include:

1. the protection of individual passwords,

2. accessing the contents of User Records i) only for a legitimate administrative or business interest as directed by contract or an Authorized Administrator, or ii) performing only the task that is specified in his or her position description,

3. avoiding direct or indirect contact with a User's personal information and communication content whenever feasible,
4. acting to ensure the uninterrupted operation of Bishop Diego Technology Resources, and

5. maintaining the safety and security of the Bishop Diego Community and Guests.

"Cloud" or Hosted Communications, Data Processing and Storage Services

All hosted or cloud-based services that provide business or communications support to Bishop Diego or that publish publicly-accessible information on the Internet must be approved and

under contract by Bishop Diego. Also, to avoid the potential loss of control of electronic communications services, all services used must be in the name of Bishop Diego and not in the name of any individual or volunteer group.

Domain Name Registration Policy

Domain name registration must be in the name of Bishop Diego, not in the name of any individual or volunteer group. The registrant and administrative contacts for all domain names must use Bishop Diego's business street address and the phone number and email address of a Teacher or Administrator designated to manage domain name registrations.

Approved by:	Board of Trustees on _
History:	Technology Committee approved: _ Amended: _ Board of Trustees approval: _ Amended: _ Revised
Related Policies:	Copyright Policy, Printer Policy
Additional References:	Employee Electronic Communications Guidelines, Copyright Guidelines
Responsible Persons/committee:	Director of Technology, Technology Committee

TABLE I - REPOSITORIES AND RETENTION PERIODS FOR RECORDS

STUDENT-RELATED ACADEMIC RECORDS

Type of Record	Official Repository	Duration
Academic files of Students	Registrar	5 years from graduation or date of last attendance
Department academic files	Department	5 years from graduation or date of last attendance
Academic Transcripts	Registrar	Permanent
Financial Aid records (applicants who do not enroll)	Admissions Office	1 year from date of application
Financial Aid records (applicants who enroll)	Admissions Office	4 years from end of fiscal year in which aid is awarded
Application Materials for applicants who do not enroll	Admissions Office	1 year from start of application term

EMPLOYMENT RECORDS

Type of Record	Official Repository	Duration
Employment files of Faculty and staff	Head of School	5 years from termination date of employee

II. COPYRIGHT POLICY

Introduction

Federal Copyright Law (Title 17 United States Code §§ 101 *et. seq.*) requires that all members of the Bishop Diego community respect the proprietary rights of owners of copyrights and to refrain from actions that constitute an infringement of such rights.

Policy

Bishop Diego's policy is for all members of the Bishop Diego Community and Guests to follow and uphold Federal Copyright Law. Users are prohibited from copying, uploading, downloading, viewing or otherwise transmitting copyrighted, trademarked, patented, or indecent materials, trade secrets, or other confidential, private, or proprietary information or materials to which the User does not have access rights.

Authorization to use Bishop Diego trademarks and logos, including any use on Bishop Resources such as the Bishop Diego official web-site, must be approved by the Director of Advancement.

Guidelines

Bishop Diego's Copyright Guidelines have been developed to assist Faculty and members of the Bishop Diego Community in complying with federal copyright law and enabling them to distinguish between permitted and prohibited uses of copyrighted materials. Members of the Community are expected to familiarize themselves with these Guidelines and to comply conscientiously with their requirements. (See Copyright Guidelines – Software Licenses, below at _)

Consequences of the User's Failure to Follow Federal Copyright Law

Administrators, Faculty, Teachers, staff, other employees and other members of the Bishop Diego Community who willfully disregard the Bishop Diego Copyright Policy place themselves in legal jeopardy and individually at risk of legal action. In the instance where a lawsuit is filed against a member of the Community, ***Bishop Diego may refuse to defend the individual named in the lawsuit***. In the course of such a lawsuit, personal liability for substantial monetary judgments, including judgments for damages, punitive damages, and attorney's fees may be entered against the employee in a federal Court of Law.

Approved by:	Board of Trustees on _
History:	Technology Committee approved: _ Amended: _

	Board of Trustees approval: _ Amended: _ Revised
Related Policies:	
Additional References:	Copyright Guidelines
Responsible Persons/committee:	Director of Technology, Technology Committee

III. PRINTER POLICY

Introduction

Faculty and staff are required to use shared, networked Bishop Diego printers (i.e., those that are connected to and can be used by more than one computer workstation.) Dedicated printers are permissible only with advance approval from the Technology Department and are subject to the requirements and limitations set forth in this policy. Departments are responsible for costs associated with printing on dedicated printers. The goal of this policy is facilitate the efficient, cost-effective use of printing and copying assets. This policy applies to anyone utilizing printing facilities provided or funded by the Bishop Diego.

Required Use of Shared Networked Printers

Shared, networked printers are provided by the Bishop Diego to facilitate the normal business operations and dedicated use by Departments. Departmental Faculty and staff are expected to use the Department's shared, networked printers for their printing and copying needs. The Technology Department will provide support for Departmental, high-volume, network accessible printers. Departments are responsible for the cost of the shared printers located in their areas.

Limited Use of Dedicated Printers

Employees whose role frequently involves the need to print Confidential Records are permitted to use a dedicated, non-networked printer. Since shared printers have a security feature enabling users to protect the privacy of their printed documents, Faculty and staff who occasionally have the need to print confidential documents will not usually need a dedicated printer. Anyone using a shared printer to print confidential documents must use that shared printer's print and release functionality.

All dedicated printers will be purchased using Departmental funds and will be exclusively maintained and supplied by the Department. The Technology Department does not support dedicated printers.

All dedicated printers will be of a brand and type specified by the Administration or Technology Department and must be purchased according to established procedures as distributed by Bishop Diego Administrators.

Confidential Bishop Records

Do not leave paper documents containing confidential Bishop Records where they are accessible to those who do not have a legitimate need to know that information. Secure all such documents in a locked suite, office, desk, or file cabinet.

Approved by:	Board of Trustees on _
History:	Technology Committee approved: _ Amended: _ Board of Trustees approval: _ Amended: _ Revised
Related Policies:	
Additional References:	
Responsible Persons/committee:	Director of Technology, Technology Committee

IV. EMPLOYEE ELECTRONIC COMMUNICATIONS GUIDELINES

These guidelines provide examples of both permitted and discouraged employee uses of Bishop Diego Technology Resources including Electronic Communications Systems. This list is not intended to be exhaustive but rather illustrative. In the event of a conflict between these Guidelines and Bishop Diego's Employee Electronic Communications Policy or the Acceptable Use Policy, the policy shall prevail.

Password security

Users are strongly encouraged to use strong passwords to access Bishop Resources and to secure personal computers; change passwords regularly to limit abuse of passwords that may have been compromised without the User's knowledge; avoid using the same password for User accounts with different providers; do not to write down passwords where they are easily accessible to others; and not to save passwords in web-browsers or send via e-mail.

Bishop Resource Access While Stepping Away From the Computer

Users should log out from Bishop Resources when finished working, or if the User will be away from their computer for more than a few minutes.

Protection of Personal Information

The best protection Users have to keep Bishop Diego from accessing private personal matters is to keep such matters off of Bishop Resources; Users should consider using Personal Resources to keep personal matters private and leave Personal Resources at home.

Personal Resource Use

Protect your Personal Resources in a case or cover when bringing them on campus, or to off-campus school activities, to avoid damage.

Incidental personal use of the Personal Devices is allowed as time permits; however, personal use of Bishop Resources should be minimal, must not interfere with operations, and must not be of a nature that could cause harm or embarrassment to Bishop Diego. Any incidental, personal use of Bishop Resources will be on employees' personal time and must not interfere

with timely performance of job responsibilities. Use of Bishop notebook computers or similar equipment at home or elsewhere off campus should reflect a similar understanding of these limits on personal use.

Legal requirements in Other Jurisdictions

Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may be subject to the laws of those other states or countries and the rules and policies on other systems and networks. Users are solely responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.

Unauthorized Access/Transfer of Financial, Student and Employee Records

All Bishop Records (including databases) that contain sensitive financial information or regarding student or employee Records are confidential. Users shall not access, modify, transmit, store or send such Records:

1. when they are collected for a specific purpose, with those outside Bishop Diego Community who do not have a Legitimate School Reason which requires knowledge of that information, without permission from an Authorized Administrator,

2. to an unauthorized recipient who does not have a legitimate administrative or business reason to possess such Records and who does not require knowledge of such Records, and

3. by facsimile (after confirming that the receiving fax machine is located in a secure area accessed only by those with a legitimate need to see the information),

without permission from an Authorized Administrator or Teacher (in the case of information about a minor), unless the User's duties or responsibilities assigned to them or set forth in their job description authorizes them to dispose of Records in the manner described above.

Inappropriate remarks or Materials

Electronic communications or Records containing insulting, disrespectful or inflammatory remarks about an individual or group's age, race, ethnicity, religion, disability, national origin,

sexual orientation, gender dysphoria and related categories are considered inappropriate and are prohibited by Bishop Diego unless such remarks are made in the context of an appropriate academic discussion, teaching or other academic activity (for example, electronic discussion of literature or history). The discussion and encouragement of traditional Roman Catholic values, morals, and principles in Ethics and Religion classes, on-campus, and at off-campus events shall not be deemed to fall within the above prohibitions.

Employees are prohibited from using Bishop Resources to download or view any type of pornography, violence, gambling or any illegal activity.

Employees are prohibited from using Bishop Resources to conduct non-Bishop Diego business, pursue hobbies or for purposes resulting in personal gain or profit to the employee.

E-mail Correspondence and Other Electronic Communications

As with paper records, proper care should be taken in creating and retaining electronic records for future use, reference and disclosure, as applicable.

Bishop Diego monitoring of Electronic Communication Resource activity

Bishop Diego, in its discretion, may also disclose the results of monitoring of Account activity, including the contents of Bishop Records and Personal Records to appropriate Bishop Diego administrators or law enforcement agencies, and may use those results in Bishop Diego disciplinary proceedings.

Under certain circumstances Bishop Diego may access and modify the contents of a Bishop Record, Personal Record, and Account. In cases concerning the health safety or welfare of Bishop Diego Community, as determined by Authorized Administrators, Bishop Diego may authorize accessing or modifying an Employee's Account. In cases where personally identifiable information has been inadvertently disclosed, Bishop Diego officials may authorize alteration or modification of the Records and/or the Accounts of both senders and recipients.

Access to email upon departure from Bishop Diego

Access to email upon departure from Bishop Diego will be in accordance with the computer Account disposition procedure. A former Employee's supervisor may request copies of Bishop Diego-related

email that arrives in the mail account as long as the account is retained. The request must be approved by the Head of School or the Director of Technology.

Approved by:	Board of Trustees on _
History:	Technology Committee approved: _ Amended: _ Board of Trustees approval: _ Amended: _ Revised
Related Policies:	
Additional References:	
Responsible Persons/committee:	Director of Technology, Technology Committee

V. COPYRIGHT GUIDELINES – SOFTWARE LICENSES

Introduction

The copyright law of the United States (Title 17, United States Code) provides legal protection for authors of original works, including literary, dramatic, musical, artistic, and other intellectual products, such as Software and computer programs.

An author's copyright in a work arises at the moment the work is created. Publication is not essential for copyright protection. The copyright symbol (©) is not required for copyright protection to occur, although use of the symbol does grant certain advantages to an author in the event of litigation.

Pertinent to Software that Bishop Diego licenses, Section 106 of the copyright law grants a copyright owner the exclusive right to do and to authorize others to do the following:

1. **reproduce** copies of the work,
2. **prepare derivative works** based on the copyrighted work, and
3. **distribute** copies of the work by sale, rental, lease, or lending or by electronic means.

Users shall not violate copyright law and must respect licenses to copyrighted materials. Unlawful file-sharing using Bishop Resources or Personal Resources is a violation of this policy. Engaging in the pirating or unauthorized use, copying, acquisition or distribution of copyrighted Software or programs is prohibited.

Licensed Works

Bishop Diego pays a fee to provide the Bishop Diego Community with online access to several databases. The databases are online at _. Different databases have different terms, conditions and features. Copyright notices must be maintained on any of the licensed materials.

Internet Technology/Computer Software

There is both civil and criminal liability for infringement of the rights of a Software copyright owner***. Copying Software without permission or without paying for a license may be a crime, even if the person copying the Software does not intend to violate the law.*** In addition, copying, installing or using an entire Software program for which a license has not

been purchased, is highly unlikely to qualify as a "fair use" of the Software, falling within the “fair use” exception of Section 107 of Federal copyright law.

Bishop Diego negotiates site licenses with selected software vendors for products that are extensively used at school, since these arrangements provide the Bishop Diego community with efficient access to computer programs that support the curriculum while assuring the copyright owner a fair royalty.

Operate on the assumption that all software is copyright-protected, even if the software has no copyright symbol. To find out if Bishop Diego has paid for a license of a software program that you would like to use, contact the Director of Technology.

Do not make copies of software or install a software program on a Bishop Diego device/computer unless either: a) permitted under a Bishop Diego licensing agreement, or b) permission is sought from the copyright owner or the program is clearly labeled "freeware" and you obtain authorization from the Director of Technology to install such software.

It may be permissible to copy software in those rare instances where it is impossible to determine who the copyright owner is. Permission must be obtained from the Director of Technology before copying or installing software whose copyright owner is unknown and cannot be determined.

While libraries are permitted to lend software in limited circumstances, Bishop Diego prohibits use, copying or installation of software borrowed from other libraries.

Specific restrictions with respect to different software vary widely. A typical form of the copyright notice on computer software is as follows:

NOTICE: Warning of Copyright Restrictions

> The copyright law of the United States (Title 17, United States Code) governs the reproduction, distribution, adaptation, public performance, and public display of copyrighted materials.
>
> Any person who makes an unauthorized copy or adaptation of this computer program, or redistributes a loaned copy, or publicly performs or displays the computer program, except as permitted by Title 17 of the United States Code, may be liable for copyright infringement.

Approved by:	Board of Trustees on _
History:	Technology Committee approved: _ Amended: _ Board of Trustees approval: _ Amended: _

	Revised
Related Policies:	
Additional References:	
Responsible Persons/committee:	Director of Technology, Technology Committee