TERMS OF SERVICE

Kent State University issues Google Apps accounts to all student employees, faculty and staff (collectively or individually referred to herein as "the user" or "you"). Google Apps is a communications and collaboration suite consisting of a core set of applications that may be used to perform both educational as well as academic and other university-related functions. *These Terms of Service do not apply to a student's personal use of Google Apps (student use is governed by Google's Terms of Service as applicable and the university's responsible use policy).*

Due to a negotiated agreement with Google, Kent State University is providing Google Apps directly to you for your use. Prior to using any of the Google Apps suite of products, you may have to individually agree to the general or specific terms of service for that particular Google App.

Kent State University reserves the right, at any time and at its sole discretion to add or remove applications and to modify the provisions of the Kent State University Google Apps services and these Terms of Services. While the University may provide notice of the addition or discontinuation of services, you as "the user" are at all times responsible for your personal information as well as any institutional data that you may have created, modified, uploaded or otherwise linked to Google Apps. The information provided in these Terms of Service explains the appropriate use of institutional data as it relates to your role at the University.

Use of Kent State University Google Apps implies you have read, understand and agree to adhere to these Terms of Service and all other applicable guidance. Failure to follow these Terms of Service or the Terms of Service provided by Google may result in suspension or termination of access to your account.

GENERAL TERMS

At all times, this Terms of Service reinforces: (1) all federal, state, local or other applicable law; (2) all university policies, regulations, and procedures; and (3) all applicable contracts and licenses.

1. When utilizing Kent State University Google Apps, you are bound by university policies 3342-9-01 and 3342-9-01.1 regarding responsible use.

2. By utilizing Google Apps, you agree to and are bound by the Google Terms of Services provided for at https://www.kent.edu/is/policies-and-procedures.

3. Any user utilizing Google Apps must be aware that any data transmitted, stored otherwise managed in Google Apps may be stored in datacenters outside the borders of the United States.

4. Users shall adhere to any and all applicable record retention schedules in place regarding any data transmitted, stored or otherwise managed under this Terms of Service. The university record retention schedules are available at: http://www.kent.edu/generalcounsel/records.

5. Any data transmitted, stored or otherwise managed in Kent State University Google Apps (as well as any other third-party provider or cloud service) may be subject to the Ohio Public Records Act, codified in Ohio Revised Code 149.43.

6. By using Google Apps, you hereby agree and provide your express consent that Kent State University may access your account for administrative and/or other purposes such as password resets and compliance with University policies governing this use or as otherwise provided for in university policies 3342-9-01 and 3342-9-01.1.

APPROPRIATE USE OF INSTITUTIONAL DATA

You may use Kent State University Google Apps to conduct University activities that are aligned with your role and the duties within the scope of your employment at the University, provided that you do so according to the University's policies on responsible use of information technology (policies 3342-9-01 and 3342-9-01.1 of the University Policy Register), and in accordance with any and all restrictions placed upon certain classifications of data and information by University policies, regulations, and/or procedures.

You are responsible for all institutional data that you transmit to, store, and manage while using Google Apps. All devices used to access institutional data must have active password protection in place and encryption where possible. The following chart is intended to provide you with a "quick glance" reference for the data categories that may be transmitted, stored or managed using Google Apps as well as in reference to other sources that may be utilized by the user. For any further clarification, please contact the Office of Security and Access Management or the Office of General Counsel.

Data Categories	**Permitted on Google Apps?**	**Permitted on Email?**	**Permitted on 3rd party or cloud services?**
Student Educational Records (FERPA)	Yes	Yes	Yes (if KSU has a contract in place)
Personal Identifying Information	No	No	No
Payment Card Industry (PCI) Information *(Credit Card Numbers)*	No	No	No
Intellectual Property	See below	See below	See below
Human Subject Research Data	See below	See below	See below
Health Information (PHI, HIPPA)	No	No	No
Financial Data (GLBA)	No	No	No
Export Controlled Data	No	No	No

<u>Family Educational Rights and Privacy Act (FERPA) Data</u>

FERPA is a federal law that protects the privacy of student education records. As provided for in our agreement with Google, Google recognizes its responsibilities under FERPA and agrees to be designated as a "School Official" for the purposes of receiving educational records during the course of providing services through Google Apps.

Users transmitting, storing or otherwise managing institutional data covered under FERPA and/or governed under university policies 3342-5-08, 3342-5-08.101, and 3342-5-08.102 shall do so consistent with the protections provided by FERPA and shall ensure that such records are disclosed (or shared) only to other parties as permitted under FERPA (i.e. the student, those who have a legitimate education-related interest, and/or those permitted by law).

Personal Identifying Information

As provided for in Ohio Revised Code 2913.49, Personal Identifying Information is an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: driver's license, driver's license number, commercial driver's license, commercial driver's license number, state identification card, state identification card number, social security card, social security number, birth certificate, employee identification number, mother's maiden name, demand deposit account number, savings account number, money market account number, mutual fund account number, other financial account number, personal identification number, password, or credit card number of a living or dead individual. Users shall not transmit, store or otherwise manage data containing personal identifying information to another user through Google Apps, Email, third-party providers, or cloud services.

Payment Card Industry (PCI) Information

The Payment Card Industry Data Security Standard (PCI-DSS) requires entities processing credit card transactions to enforce stringent security requirements for stored credit card information. These requirements apply to all entities transmitting or otherwise managing credit card information. Cardholder data is defined as the full magnetic stripe or the Primary Account Number (PAN) plus any of the following: cardholder name, expiration date, and service code. Users shall not transmit, store or otherwise manage data containing PCI information to another user through Google Apps, Email, third-party providers, or cloud services unless otherwise provided for in accordance with university policy 3342-7-12.

Intellectual Property – Collaboration Use

User may utilize collaboration tools available in Google Apps or other applications to view data, co-edit documents, etc. It is the responsibility of each user to ensure that the appropriate sharing controls and protections are used in order to protect Kent State University intellectual property or third-party confidential intellectual property provided to the University under contractual terms requiring non-disclosure.

Human Subject Research Data

Human Subject Research data is a body of personally identifiable data elements collected in the course of research with living human beings. Human Subject Research regulations require adequate protections to protect the privacy of subjects and to maintain the confidentiality of data to limit access from external third parties, including third-party vendors contracted with the University. In accordance with 45 CFR 46.111(a), users should address the use of Google Apps, Email or third-party providers, or cloud services in relation to the “adequate provisions to protect the privacy of subjects and to maintain the confidentiality of the data” in the research proposal before proceeding.

Health Information – Health Insurance Portability Accountability Act (HIPAA) and Protected Health Information (PHI) Data

HIPAA is a federal law that protects the security and privacy of individuals' health data. Users shall not transmit, store or otherwise manage data containing HIPAA-protected or PHI information to another user through Google Apps, Email, third-party providers, or cloud services.

Financial Data (Gramm-Leach Bliley Act – GLBA)

The Gramm-Leach-Bliley Act (GLBA) includes provisions to protect consumers financial information held by financial institutions. The University is obligated by federal regulation to protect this data. Communication of financial aid or payment of fines may be subject to GLBA requirements. Users shall not transmit, store or otherwise manage data containing GLBA-protected information to another user through Google Apps, Email, third-party providers, or cloud services.

Export Controlled Data

There are several existing federal restrictions on data that has been designated as export control data (for example, export control laws restrict the export of goods and technology, thereby, ensuring protection of United States national security and trade). Users shall not transmit, store or otherwise manage data containing export-controlled data to another user through Google Apps, Email, third-party providers, or cloud services. For further information on export control laws, go to the Office of Sponsored Programs resource page at: https://www.kent.edu/sponsored-programs/federal-funding-policies-compliance

APPLICABLE LAWS AND POLICIES

You agree not to use the provided Google Apps intentionally or unintentionally to violate any applicable law.

BREACH AND/OR VIOLATION

You agree that in the event you are aware that a breach has occurred, or has likely occurred, you must notify the Office of Security and Access Management immediately at 330-672-5566 or by email at security@kent.edu.

If the University receives a credible report that a violation of these Terms of Service has occurred, or if, in the course of managing the service, discovers evidence of a violation, then the matter will be referred for investigation, disciplinary action according to university policies, and/or criminal prosecution.

CHANGES TO THE TERMS OF SERVICE

Kent State University reserves the right to change this policy at any time. The University will post the most up-to-date version of the policy on the University website at https://www.kent.edu/is/policies-and-procedures and may, at its discretion, provide users with additional notice of significant changes. A user's continued use of Google Apps after any changes are published binds the user to the revised policy.