KERN COUNTY PROBATION DEPARTMENT
Policies And Procedures

TITLE: **Electronic Mail Acceptable Use**			Article: 1507
APPROVED: **William Dickinson, Chief Probation Officer**			
EFFECTIVE: October 2016	REVIEWED: September 2018	REVISED: September 2024	UPDATED: September 2018

POLICY

IN CONJUNCTION WITH THE KERN COUNTY ELECTRONIC COMMUNICATIONS USAGE POLICY.

The purpose of this policy is to ensure the proper use of the Kern County Probation Department's email system located on Department servers and used by Department staff. Electronic Mail is a tool provided by the Department to complement traditional methods of communication and to improve administrative efficiency. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. Use of the Department Email Accounts evidences the user's agreement to be bound by this policy. Violations of the policy may result in restriction of access to Department Email Accounts and/or other appropriate disciplinary action.

I. ACCOUNT CREATION

Department Email Accounts are created based on the official name of the staff reflected in Payroll records. Requests for mail aliases based on name preference, middle name, nicknames, etc., cannot be accommodated. Only requests for name changes to correct a discrepancy between an email account name and official Department records will be processed, in which case the email account name will be corrected. User id's will remain in the Department's system and will not be reused at any time.

II. OWNERSHIP OF EMAIL DATA

The Department owns the Department Email. This means that the Department Email is subject to underlying copyright and other intellectual property rights under applicable laws and Department policies, the Department also owns data transmitted or stored using the Department Email Accounts.

III. PERSONAL USE

A. While incidental personal use of a Department Email Account is acceptable, conducting business for profit using a Department Email Account is forbidden.

B. Use of a Department Email Account for political activities (supporting the nomination of any person for political office or attempting to influence the vote in any election or referendum) is forbidden.

C. Any use of a Department Email Account to represent the interests of a non-Department group must be authorized by the Chief Probation Officer or their designee.

IV. PRIVACY AND RIGHT OF DEPARTMENT ACCESS

While the Department will make every attempt to keep email messages secure, privacy is not guaranteed, and users should have no general expectation of privacy in email messages sent through a Department Email Account. Under certain circumstances, it may be necessary for the IT staff or other appropriate Department officials to access Department Email Accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security or abuse incidents, or investigating violations of this or other Department policies. Department officials may also require access to a Department Email Account in order to continue Department business where the Department Email Account holder will not or can no longer access the Department Email Account for any reason (such as death, disability, illness or separation from the Department for a period of time or permanently). Such access will be on an as-needed basis and any email accessed will only be disclosed to those individuals with a need to know or as required by law.

V. DATA PURGING AND RECORD RETENTION

A. Individuals are responsible for saving email messages as they deem appropriate. Unless a legal hold has been placed on an account, messages in Department Email Accounts are automatically purged from folders as follows:

1. Inbox – 90 Days – Then moved to Archive.
2. Sent / Sent Items – 90 Days – Then moved to Archive.
3. Trash / Deleted Items – 30 Days.
4. Junk / Junk Email – 30 Days.

B. Due to finite resources, the Department has the right to restrict the amount of user space on the Department Email Accounts as necessary, to revise the above purge policies with appropriate approval and advance notice, and to purge and remove Department Email Accounts of any staff remaining on the Department's email system who have not accessed their account for 90 days or more. Email retention is two years.

C. It is the responsibility of employees who have actual knowledge of matters in which it can be reasonably anticipated that a court action will be filed, a

subpoena has been served or notice of same has been given, or records are sought pursuant to an audit, a government investigation or in similar circumstances to attempt to preserve Department records, including emails or instant messages.

VI. DATA BACKUP

The Department Email Accounts are backed up on a regular basis as a way of recovering from a systematic loss impacting the entire email system. User files and folders are not backed up individually, and the IT staff cannot accommodate requests to restore these files or folders. While in some cases it may be possible to recover from the accidental deletion of files by a user, this is generally not feasible, and therefore each email user is responsible for backing up individual messages and folders as appropriate.

VII. APPROPRIATE USE

When using email as an official means of communication, staff should apply the same professionalism, discretion, and standards that they would use in written business communication. Staff should not communicate anything via email that would not be prepared to say publicly. Users of email shall not disclose information about employees in violation of Department or County policies or laws protecting the confidentiality of such information. No private personally identifiable information about staff should be transmitted via email or stored in an unencrypted format. Use of distribution lists or 'reply all' features of email should be carefully considered and only used for legitimate purposes as per these guidelines.

VIII. USER RESPONSIBILITY

A. Technology Services maintains the Department's official email system. Staff are expected to read email on a regular basis and manage their accounts appropriately.

B. Sharing of passwords is strictly prohibited unless otherwise directed by Management. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is deemed to be authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.

IX. SUPPORTED MAIL CLIENTS

A. Department supported email clients are GroupWise 8 and GroupWise Web Access. Technology Services is continually evaluating tools and

technologies and reserves the right to modify the list of supported clients with appropriate notification.

X. INAPPROPRIATE USE

A. Any inappropriate email usage, examples of which are described below and elsewhere in this policy, is prohibited. Users receiving such email should immediately contact Technology Services, who in certain cases may also inform the proper authorities.

B. The exchange of email content that:

1. Generates or facilitates unsolicited bulk commercial email;

2. Infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;

3. Violates, or encourages the violation of, the legal rights of others or federal and state laws;

4. Is for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;

5. Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;

6. Interferes with the use of the email services, or the equipment used to provide the email services, by customers, authorized resellers, or other authorized users;

7. Alters, disables, interferes with or circumvents any aspect of the email services;

8. Tests or reverse-engineers the email services in order to find limitations, vulnerabilities or evade filtering capabilities;

9. Constitutes, fosters, or promotes pornography;

10. Is excessively violent, incites violence, threatens violence, or contains harassing content;

11. Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;

12. Improperly exposes trade secrets or other confidential or proprietary information of another person;

13. Misrepresents the identity of the sender of an email;

14. Is otherwise malicious, fraudulent, or may result in retaliation against the Department by offended viewers.

C. Other improper uses of the email system include:

1. The use or attempt to use the accounts of others without their permission. Collecting or using email addresses, screen names information or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting);

2. Use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;

3. Any conduct that is likely to result in retaliation against the Department's network or website, or the Department's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS).

4. Electronic signatures containing tag lines are prohibited.

D. These guidelines provide some examples of permitted or prohibited use of email. This list is not intended to be exhaustive but rather to provide some illustrative examples.