Electronic Communications

306.1 PURPOSE:
To establish guidelines for Probation Department employees/volunteers regarding the use of electronic communication systems, telephones, mobile devices, file hosting services, web-based systems, electronic communication, and the Internet.

306.2 DEFINITIONS:
Confidential Data: Information about the clientele, casework, criminal or gang intelligence, disaster recovery, crisis response, multi-agency operational planning, NIMS planning, training information (PowerPoint presentations, handouts, etc.), personnel, evidence, an investigation, or data otherwise accessible only by subpoena.

Electronic Communication: Any transfer of signs, signals, writing, images, sounds, data, information, or intelligence transmitted by a wire, radio, electromagnetic, photo-electronic, or photo-optical system including, but not limited to, facsimiles, removable storage, mobile devices, file hosting services, web-based systems, and the Internet as it relates to the Probation Department.

Internet and Electronic Communications Agreement (Attachment A): Agreement which outlines employee responsibilities regarding the use of County/Department owned or approved electronic communication systems, removable storage, mobile devices, file hosting services, web-based systems, electronic communication, social media, and the Internet.

Information System (IS): A system composed of people, computers, software, data, and procedures used to run a computerized database that processes/interprets, collects and stores information to support operations, management, and business processes.

Removable Storage Media (RSM): Any form of data storage that is not incorporated into the computer itself.

Social Media: Host file services (Facebook, Twitter, Instagram, etc.) that allow members to collectively communicate, view, and share information, photos, video, audio, text, data, multimedia files, etc., through interlinked networking accounts.

Telephones: Includes telephone instruments, cellular telephones, and other electronic communication equipment owned, leased, or rented by the County.

306.3 RESPONSIBILITIES:

I. All Staff/Volunteers:

A. Every employee/volunteer is considered an agent of the County of San Bernardino and the Probation Department in regards to any transaction or electronic communication produced through County owned computer systems and will make every effort to protect the interests of the County and the Probation Department.

B. Telephone:

1. Occasional personal use of telephones is allowed, but such usage shall not violate any existing law, regulation, County policy, departmental or personnel rules. Nor shall personal use interfere with the conducting of County business or interfere with the performance of an employee's duties.
2. Any toll charges incurred from personal use shall be reimbursed to the County using appropriate departmental procedures.
3. Unit supervisors are responsible for monitoring the phone use on their unit and areas of supervision.

C. Internet:

1. Use of the County internet resource streamlines work load while maximizing productivity and services. Every effort must be made to protect the confidentiality, maintain a professional manner, and prohibit inappropriate, explicit, or illegal activity.
2. In general, staff must not use County systems or networks for personal activities. However, reasonable incidental (de minimis) personal use of County resources, such as internet access and email, is allowed as long as such use does not violate the County's acceptable use policies, does not interfere with the performance of work duties, or the operation of the County's information systems. If staff are unclear as to what is considered appropriate incidental personal use, it is their responsibility to request clarification from a supervisor.
3. Occasional personal use of the internet resources provided by the County is allowed, when not on county work time, however, unrestricted use for non-County business is not permitted.

D. Electronic Communication:

1. Email is covered by the Electronic Communications Privacy Act, 18 USC SS 2510-2521 and is legally privileged.
2. Utilization of email to distribute, for example, offensive, abusive, threatening, pornographic, or hate messages is prohibited. Any Probation Department employee who receives such an email shall immediately notify their supervisor.
3. Confidential material in electronic format shall only be sent using internal County e-mail/webmail.
4. Email Encryption shall be used in order to protect Personal Identifiable Information (PII) or Protected Health Information (PHI) when email is being sent to an address external to the County.
5. Any data on disaster recovery, crisis response, multi-agency operational planning, NIMS planning, criminal intelligence, or other information to be shared between agencies may be transferred using RSM's, providing the

RSM is securely transported and in the control of personnel from either/ or both agencies at all times.

E. Shall not store personal photographs on Department computers or drives.

F. Social Media:

1. Staff are prohibited from:

(a) Posting photographs taken of them or any other staff in their Department issued duty attire and/or gear to personal social media sites.

(b) Listing, describing, or disclosing confidential or operationally sensitive information or the personal information, including photographs, of other members of the Department.

G. Shall read and sign the Internet and Electronic Communications Agreement form (Attachment A).

H. Shall submit a completed Computer Sign-on Request (CSOR) form (Attachment B) to their supervisor.

I. There is no expectation of privacy for users of county resources (telephone, internet, electronic communications, etc.) and/or equipment.

II. Professional Standards:

A. Shall work in conjunction with Automated Systems to obtain any identified data for review (e.g., email, internet, "U" drive, local computer storage, etc.).

306.4 ATTACHMENTS:

See attachment: Electronic Communications Attachment A (Lexipol 4-13-22).pdf

See attachment: Electronic Communications Attachment B (Lexipol 4-13-22).pdf

Attachments

Electronic Communications Attachment A (Lexipol 4-13-22).pdf

SAN BERNARDINO COUNTY
PROBATION DEPARTMENT

Internet and Electronic Communications Agreement

Employment/volunteering with the Probation Department may involve the use of county computers, email, voice mail, removable storage, mobile devices, file hosting services, web-based systems, Internet, facsimiles or other forms of electronic communications and/or systems. In order to ensure all individuals who use the items listed above do so in a lawful, ethical, and proper manner, this agreement sets forth specific expectations concerning applicable rules to protect business, staff and client interests.

Security:

1. It is important to exercise care when sending or receiving sensitive, privileged, proprietary, or confidential information.
2. Unauthorized alteration or destruction of computer hardware, software, or data may result in disciplinary action up to and including, termination of employment or release as a volunteer and may additionally result in prosecution in accordance with applicable federal and state laws.
3. No software may be introduced into the system without the approval of a Director and the Business Applications Manager/Designee.
4. Passwords are digital fingerprints recognized as your legal signature. As such, you are accountable for all work, transactions, or communications performed under your password.
5. Do not disclose your password to anyone or use another's password.
6. If you believe your password has been compromised notify your supervisor immediately and change your password.
7. The Probation Department reserves the right to access any information received on, transmitted by or stored in any County owned computer, mobile device, removable storage media, file hosting services, web-based systems, Internet, facsimiles electronic communications or voice mail systems either with or without the employees/volunteers consent.

Confidentiality:

1. Information stored electronically (client, staff, etc.) is confidential information and must be treated with the same care as information in paper files.
2. Confidential information included in email must be given the same security as case files, personnel documents and other confidential material.
3. Information Systems and specific electronic communications (intelligence, officer safety issues, etc.) fall under need-to-know restrictions. Access to the information must be necessary for the conduct of one's official duties.
4. Report any electronic confidentiality breaches or suspicions of such to a supervisor.

Internet:

1. In general, staff must not use County systems or networks for personal activities. However, reasonable incidental (*de minimis*) personal use of County resources, such as internet access and email, is allowed as long as such use does not violate the County's acceptable use policies, and does not interfere with the performance of work duties or the operation of the County's information systems.
2. Access through the Department server/network while on duty, shall be reasonable, not violate prohibited activities or interfere with probation business or duties.

3. Any activity that may be a violation of the County of San Bernardino Internet/Intranet Use Policy #09-04, or the Departmental Conflict of Interest and/or Confidentiality policies is prohibited.
4. Accessing offensive websites or those that contain objectionable material such as pornography or discriminatory material as referenced in the County of San Bernardino Electronic Mail (e-Mail) systems Policy #09-01 is strictly prohibited. The exception to this is employees in specialized assignments, which necessitate accessing these sites. The employee must have approval from his/her immediate supervisor before accessing these sites.

Electronic Communication:

1. Email shall be used for business purposes. Limited occasional or incidental use of email for personal purposes may be acceptable if done in a professional and appropriate manner, not used on County work time, not violating prohibited activities and not interfere with probation business or duties (SBC Policy #09-01).
2. Email generated via the Department server/network includes a confidentiality statement pursuant to the Electronic Communications Privacy Act, 18 USC SS 2510-2521.
3. All emails are expected to reflect a professional tone without the use of profanity, gossip or derogatory language.
   a. Email shall include ONLY the name, title, location, assignment and telephone number in the "signature" portion. Quotations, tag lines, or any other information not directly related to the user's county identifying information is prohibited.
   b. Utilize the out of office email reply when out of the office for vacation, training, work at home, scheduled day off etc. Be sure to include a timeframe outlining your dates of absence, expected return and unit supervisor and clerk name and phone number.
4. When on duty, staff are required to check all incoming email at least once each working day. As such, urgent matters should not be sent via email.
5. All email communications are automatically stored and are subject to review by Probation Department management without notice.
6. Do not engage in the unreasonable personal use of Department electronic communications while on duty, violate prohibited activities or interfere with probation business or duties.
7. Electronic communication shall not contain animation, specialized graphics, colored wallpaper or backgrounds.
8. Do not communicate messages that would constitute unlawful or sexual harassment, sexually offensive material or information, or use offensive screen savers.
9. Do not violate trademark, copyright, intellectual property rights or license rights (software or otherwise).

Encryption:

1. Employees and contractors of the Probation Department utilizing the County's prob.sbcounty.gov email system who have a business need that requires sending confidential data, that may include Personal Identifiable Information (PII) or Protected Health Information (PHI), to an email address that is external to the County shall use a method to send the email that includes data encryption.
2. Employees and contractors shall not place confidential information in the "Subject" line of any email message.

3. Employees and contractors that receive confidential information from a citizen by email shall not reply to the message unless they utilize encryption or remove the confidential information from the reply message.
4. Employees and contractors that receive confidential information from a citizen by email that is listed in the "Subject" line of the message will redact the information from the "Subject" line prior to replying and use encryption as appropriate.
5. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.
6. Staff are encouraged to reference County of San Bernardino Standard Practice 14-03 SP03 and SP07 for further details.

Social Media:

1. Any staff member who chooses to participate in social media or social networking platforms shall conduct themselves in a manner that will not reflect negatively upon the Department or its mission.
2. Access to the Department website and social media sites via the Department's computer network while on duty is acceptable, based on an organizational need to do so and with the approval of the employees' supervisor.
3. Do not engage in the unreasonable personal use of Department computers or access to the Department website/social media sites, personally maintained social media sites or other organizational websites while on duty.
4. Staff shall not post, publish, forward, or display any text, photograph, audio file, video file, or any other media format on any personal social media or networking site, blog, commentary, or news site, that may be reasonably foreseen to bring discredit to themselves or the Department, be construed as indecent, lewd, offensive, be intermingled with other posts that would bring discredit to the employee or the Department or compromise the professional integrity of the Department.
5. Any on or off duty use of internet or social media and networking sites shall not be used in any manner which could be reasonably foreseen to be detrimental to the Department, its operations, or be a danger or threat to staff. This includes, but is not limited to:
    a. Posting personal or Department photographs taken of them on-duty to personal social media sites.
    b. Listing the Department as their employer (to include their rank, job classification and assignment). Employee work schedules, detention corrections security measures, youth transportation arrangements, criminal intelligence/officer safety briefs, or other operationally-sensitive information.
    c. Display of Department graphics, emblems, insignias, logo uniforms, patches, badges, equipment, vehicle, or facilities in a negative manner or weapons if displayed or depicted in such a manner that it promotes or glorifies violence.
    d. Descriptions or discussions of Department enforcement methods, procedures, tactics, training, equipment, organizations, or staffing.
    e. Information or opinions regarding a Department administrative or criminal investigation, arrest, enforcement action, or pre-sentence investigation.
    f. Information that staff has been restricted from divulging by an administrative order of confidentiality.
    g. Information or opinions regarding the case work, investigation, detention practices, or administrative actions of other Department personnel.
    h. Comments solely meant to discredit the Department, other law and justice professionals, agencies, or members of the judiciary.
    i. Confidential information accessed or known by the member as a result of their status, rank, position, or assignment within the Department.

j. Addresses, phone numbers, or other personal information of members of the Department.

Electronic Equipment:

1. Each employee/volunteer is responsible for the equipment made available to them. Employees may be expected to reimburse the Department; if it is determined lost or damaged equipment is the result of gross negligence or a dishonest or willful act.
2. All equipment issued to an employee/volunteer must be returned to the Probation Department upon separation from service.

I understand that any violation of the above agreement may result in disciplinary action, up to and including termination of employment or release as a volunteer.

I have been provided the opportunity to ask questions pertaining to the above agreement.

I have read the above agreement, understand it, and agree to abide by it.

Employee/Volunteer Signature	Employee ID
Employee/Volunteer Name (Print)	Date
Supervisor Signature	Employee ID
Supervisor Name (Print)	Date

Distr bution:
Original – Probation Personnel Office (Employee's Personnel File)
Copy – Employee

Electronic Communications Attachment B (Lexipol 4-13-22).pdf

PROBATION DEPARTMENT
COMPUTER SIGN-ON REQUEST FORM (CSOR)

Contact Name: **Date:**

Supervisor Name: **Supervisor Phone:**

Automated Systems will only process forms that are completed and signed. Forms that do not include all required signatures will be returned to the requestor. Please allow up to 72 hours (after all necessary signatures are obtained) for your requests to be processed.

Interoffice completed forms to: Automated Systems, mail code [redacted]

USER INFORMATION	☐ **Existing Employee**	☐ **New Employee**	**Start Date: _____**
Employment Type: ☐ Employee ☐ Temp ☐ Other Type (Specify):			**Employee ID:**
LEGAL Name (Last, First): LastName, FirstName			**Phone#:**
Position Title:		**Primary Site Assigned: (Click here to select an option)**	

PLEASE CHECK ACCOUNT(S) REQUESTED

☐ **Windows Network Acct & E-Mail** *(new account requests only)*

☐ **E-mail Distribution Groups membership** *(Please specify NAME, as it appears at the top of an e-mail):*

Dist. Grps:

☐ **Shared Folders** *(Example; drive letter + Location, i.e.: X:\\prb-data\Placement):*

☐ **Internet - (Click here to select an option)** *←(Access to county web sites, other government sites, and Google services DOES NOT REQUIRE Internet access)*

☐ **CE -** Provide the name/Emp ID of a person in a similar position to emulate. **Name:**			**Empl #:**
☐ **eCase eXchange**	☐ **PETS**	☐ **Transcription Service**	☐ **Policy Manager for DBH Employees**

☐ **SO/JIMs Access** *(Submit a separate Sheriff Clearance Form, also located in Prob Tools)Not available for Volunteeers.*

☐ **Desktop CAD Access:** *(Requires Admin Review – For Supervisors with field staff ONLY.)*

☐ **JNET** (**Please include JUSTIFICATION; i.e.: What can they see or do in JNET that they cannot in CE**):

☐ **TechCare** *(Requires approval by [redacted])* ☐ **CIPS** *Signature:* Provide the name/Emp ID of a person in a similar position to emulate. **Name:** **Role(s):**	_____

The following accounts are not processed by Automated Systems. Please contact the person listed on the dropdown: (Click here for contact information)

Unit Supervisor's Signature:	**Date:**____/____/____
Division Director's Signature (Only required for Standard Internet access):	**Date:**____/____/____
DCPO's Signature (Only required for Unrestricted Internet access)::	**Date:**____/____/____

AUTOMATED DEPT. USE ONLY

☐ **Accts Created:**

☐ **Entered in Account Tracking Database** _____/_____/_____

☐ **Contact/User Notified via Email**	☐ **Processed By:**