	Tennessee Department of Children's Services **Protocol for DCS Shared Email Accounts and Distribution Groups**
	Supplemental to DCS Policy: Chapter 7

This protocol addresses the creation, management, and appropriate use of Department of Children's Services (DCS) shared email accounts and distribution groups to ensure these shared accounts and groups are used in accordance with their intended purpose, which is to support operational efficiency, professionalism, and appropriate communication standards across the organization. This protocol is applicable to all employees with access to DCS shared email accounts and distribution groups.

A. Creation of Shared Email Accounts and Distribution Groups

To maintain consistency, security, and appropriate use, all new shared email accounts or distribution groups must be requested and approved through the designated process.

1. Request Process

   a) Submit a formal request to the Strategic Technology Solutions (STS) DCS Information Technology (IT) Access Management team via ServiceNow using the following link: **Change User Account Access - Children's Services Service Portal** or by calling STS DCS IT Help Desk at 615-741-4636 / toll free 888-853-4636.

   b) All requests must include the information listed below.

   - The purpose of the account or group.
   - The Region or Program Area it supports.
   - A list of authorized supervisors and users (with role-based justification).
   - The proposed email address or group name.
   - Requests must be reviewed by a Regional or Program Director.
   - The Regional or Program Director will send to their Executive Director for final approval.

2. Shared Email Accounts

   a) Shared email accounts must adhere to the below configuration requirements.

   - Appropriate naming conventions (no acronyms).
   - Clearly defined permissions (Send As, Send on Behalf, Read-Only, etc.).
   - Security settings aligned with data classification (e.g., approved for Personally Identifiable Information (PII)/Personal Health Information (PHI) if necessary).

3. Distribution Groups

   a) All distribution groups must:

- Have a clearly documented owner.
- Be updated regularly to reflect staffing and/or role changes.

B. Ongoing Management and Oversight

Shared email accounts and distribution groups must be actively managed to ensure they remain secure, accurate, and aligned with organizational needs.

1. Account Ownership & Responsibility

   a) Each account or group must have a designated Account Owner (Director level or higher).

   b) The Account Owner is responsible for the following tasks:

   - Maintaining a list of authorized users.
   - Reviewing access quarterly to ensure accuracy.
   - Reporting changes in staffing or function to IT for updates.

C. Monitoring & Compliance

1. Account usage may be monitored or audited by STS to ensure adherence to policy.

2. DCS leadership and STS will review annually to audit usage.

D. Inactivation & Decommissioning

3. Functional email accounts or distribution groups that are no longer in use must be:

   a) Reported to IT for deactivation.

   b) Properly archived or deleted based on data retention policies.

   c) Communicated to stakeholders to avoid disruption.

   d) Removed from policy, as applicable, prior to deactivation.

E. Intended Uses

1. DCS shared email accounts and distribution groups must be used only for the business function or purpose for which they were created. Personal use or use beyond the assigned operational scope is prohibited.

F. Authorized Users

1. Only supervisors and designated staff members with a legitimate business need may send communications to and from a DCS shared email account and distribution group. Access must be approved by the relevant program supervisor or department head.

G. Email Distribution Best Practices

1. When sending bulk communications to a DCS distribution group, especially announcements or notices where replies are not needed or desired, employees should do the following:
   a) Place distribution group email address in the **Bcc (Blind Carbon Copy)** field.
   b) Use a neutral address (e.g., senders individual DCS email address) in the **To** field.
   c) This prevents reply-all responses and limits unnecessary email chains.
   d) If appropriate, configure an auto-reply message on the DCS shared email account or distribution group stating: *"This mailbox is not monitored. Please do not reply to this message."*

H. Confidentiality, Data Protection, and Secure Transmission of Information

1. DCS Employees are responsible for protecting sensitive information and must take appropriate precautions when sending or receiving content through DCS shared email accounts and distribution groups.
   a) Type of sensitive information includes the following:
      - Personally Identifiable Information (PII): This includes child and/or family names, social security numbers, addresses, birthdates, and other identifying details.
      - Protected Health Information (PHI): Any information covered under the **Health Insurance Portability and Accountability Act (HIPAA)**.

2. Guidelines for Handling PII and PHI

Do not send PII or PHI through a shared email account or distribution group unless the following conditions are met:

a) The DCS shared email account and/or distribution group is approved by a Regional Executive Director or program area Executive Director.

b) It is essential to the job function and program area to email PII and PHI.

c) All recipients are authorized and have a business need to access that data.

d) The sender includes, and is required to include the following statements in the subject line and in the body of the email:

- Subject line: (Includes PII/PHI)
- Bottom of email: **NOTE: This email may contain PRIVILEGED and CONFIDENTIAL information and is intended only for the use of the specific individual(s) to whom it is addressed. If you are not an intended recipient of this email, you are hereby notified that any unauthorized use, dissemination or copy of this email or the information contained in it or attached to it is strictly prohibited. If you have received this email in error, please delete it and immediately notify the person named above by reply mail.**

e) All emails containing PII or PHI are, and must be, encrypted.

- Use Microsoft Outlook's built-in encryption tools by selecting "Encrypt" before sending.
  - For Distribution Groups, the plus (+) sign to the left of the group name must be clicked to allow all recipient names in the group to show in the "To" line of the email. If the plus (+) sign is not clicked, recipients of the email will not be able to open the contents the encrypted email.
- If you are unsure how to encrypt an email, consult IT or program leadership.
- Do not forward or copy sensitive information from encrypted messages into unencrypted ones.

f) The amount of sensitive data shared is limited to the minimum necessary information.

g) Recipient lists are double-checked prior to sending to ensure sensitive data is not inadvertently disclosed to unauthorized users.

3. Security and Access Considerations

   a) It's highly encouraged that DCS supervisors and staff create internal SharePoint sites to reduce risk of unintentional exposure of sensitive data. Supervisors can determine access rights for users (read, write, admin).

   b) Be aware that DCS shared email accounts and distribution groups are often accessed by multiple users. This increases the risk of unintentional exposure of sensitive data.

   c) Report any suspected misdirected email immediately to your supervisor.

I. Reply Etiquette

1. "Reply All" should be used only when all recipients genuinely need to be informed or involved.

2. DCS Employees must exercise discretion to minimize excessive and unnecessary email traffic.

3. Avoid using distribution groups for informal, non-essential discussions.

J. Tone and Content

1. Communications sent through a DCS shared email account and distribution groups must maintain a professional tone and reflect the collective voice of the team or department it represents.

K. Oversight

1. Usage of DCS shared email accounts and distribution groups may be monitored. Misuse, including off-topic replies, unprofessional tone, or using the account outside its designated scope, may result in access restrictions and/or disciplinary action.

L. Enforcement

1. Violations of this business rule will be addressed in accordance with the organization's disciplinary policies and may include revocation of access or further corrective action as appropriate.