



ORIGINALS WITH SIGNATURES ON FILE AT STATION 1



SOUTHERN PARK COUNTY FIRE PROTECTION DISTRICT

Guffey, Colorado • Established 1987

1745 County Road 102, Guffey, CO 80820 • (719) 689-9479 • www.guffeyfire.net

This is a public policy document of the Southern Park County Fire Protection District. Copies are available at Station §1 and at www.guffeyfire.net.

POLICY NO. 200-2.04

CONFIDENTIALITY AND NON-DISCLOSURE

Southern Park County Fire Protection District • Series 200 — Governance & Administration

Policy Number:	200-2.04	Document Number:	20260408_ADMIN_200-2.04_ConfidentialityNonDisclosure_DRAFT-v0.4
Effective Date:	May 12, 2026	Adopted:	May 12, 2026
Reviewed / Revised:	—	Next Review:	Annual — Q1 each year
Approved By:	Board of Directors, SPCFPD	Classification:	PUBLIC POLICY DOCUMENT
Supersedes:	Portions of Legacy Policy #030 (Release of Information, 2012) — as to confidentiality obligations of District personnel. The February 2026 confidentiality draft (20260218_ADMIN_200-2_12_Confidentiality_DRAFT_v0_1.docx) is incorporated into this policy and is superseded as a separate draft document.		
Cross-References:	BAM v1.1 (§§ 2.3.3, 9.1.3) • Policy 100-1.02 (Mission, Core Values & Ethics § 5.3, 5.7) • Policy 200-2.01 (Code of Ethics §§ 5, 12) • Policy 200-2.12 (CORA Compliance Procedure) • Policy 200-2.11 (Records Retention) • Policy 200-2.13 (Citizen Complaint Procedure) • Policy 300-3.13 (Progressive Discipline — pending) • C.R.S. § 24-6-402(2)(d.5) (Executive Session Recordings) • C.R.S. § 24-72-201 et seq. (CORA) • HIPAA 45 C.F.R. Parts 160, 164 • C.R.S. § 24-18-101 et seq. (Colorado Government Ethics Act)		

1. PURPOSE

Effective governance and safe operations require that certain information be shared only with those who have a legitimate need to know it. The District receives, creates, and maintains information that — if disclosed prematurely, carelessly, or without authorization — could harm individuals, compromise ongoing operations, undermine public trust, expose the District to legal liability, or impair the Board’s ability to deliberate freely.

This policy establishes the District’s confidentiality and non-disclosure framework: what information is confidential, who owes the duty, how long the duty lasts, the operative rules for protecting confidential



information in daily practice, the relationship between this duty and the public's right of access under CORA, and the procedures for responding when a breach occurs or is suspected.

Relationship to other policies. Policy 200-2.01 §§ 5 and 12 establish confidentiality and social media as enforceable conduct principles; this policy provides the definitions, categories, and operative rules that implement those principles. BAM § 2.3.3 establishes the Director-specific confidentiality obligation and controls as to Director governance conduct; this policy supplements it for all personnel. Policy 200-2.12 establishes the District's CORA compliance procedure; this policy addresses the confidentiality side of the same framework.

2. SCOPE

This policy applies to all persons associated with the District in any capacity, including all Directors, the District Chief and all paid staff, all active volunteers and reserves, contractors and agents acting on behalf of the District, and advisory body members. The confidentiality duty applies whenever a person receives, creates, accesses, or becomes aware of confidential information in connection with their District role, regardless of the medium — oral, written, electronic, or incidental observation.

- a. **Duration of duty.** The confidentiality duty begins on the first day a person performs any function for the District, including orientation. It continues for the duration of service and, for categories of information designated as permanently confidential (executive session content, attorney-client communications, and patient records), survives the end of service indefinitely. For other categories, the post-service duty continues for as long as the information remains non-public. See also Policy 200-2.02 § 10 (Post-Service Obligations).
- b. **Contractors and temporary personnel.** Contractors, vendors, and temporary personnel who are granted access to confidential District information shall be informed of this policy before that access is granted. Significant access shall be documented by a confidentiality acknowledgment in the applicable contract or engagement letter.

3. DEFINITIONS

"Confidential Information." Information that: (i) is exempt from public disclosure under a specific provision of the Colorado Open Records Act (C.R.S. § 24-72-204) or other applicable law; (ii) involves the personal privacy of an identified individual in a way that reasonable persons would recognize creates a legitimate expectation of privacy; (iii) has been designated as confidential by the Board; or (iv) falls within one of the categories listed in § 4. Information that is already in the public domain — including all adopted District policies, Board minutes once approved, and meeting agendas as posted — is not confidential information for purposes of this policy.

"Need to Know." A person has a "need to know" confidential information if they require it to perform a specific function assigned to them in their District role and they would be unable to perform that function effectively without it. Curiosity, general interest, and supervisory status alone do not establish need to know. The District Chief determines need to know for operational personnel. The Board Chair determines need to know for Director access to governance information.

"Authorized Disclosure." A disclosure of confidential information that is: (i) required by Colorado law or federal law (including CORA responses, court orders, or mandatory reports); (ii) approved by the Board by majority vote at a duly noticed meeting; (iii) made by the District Chief or Board Chair for legitimate operational or governance purposes within their respective authority; or (iv) made by a specific person expressly authorized to make that disclosure by the Board or District Chief.

"Breach." Any disclosure of confidential information that is not an authorized disclosure. A breach includes intentional disclosure, negligent disclosure, and disclosure resulting from failure to take reasonable precautions. An inadvertent disclosure is still a breach, even if no disciplinary action results.

"Pre-Decisional Information." Information that reflects the Board's or District Chief's deliberative process before a final decision is made, including draft policies, preliminary recommendations, internal analyses, and working documents. Pre-decisional information is confidential until a final decision is publicly announced or a document is formally adopted. See C.R.S. § 24-72-202(6)(b).



4. CATEGORIES OF CONFIDENTIAL INFORMATION

The following ten categories constitute confidential information for purposes of this policy. The examples in each category are illustrative, not exhaustive. Where a category is confidential “by law,” that protection exists whether or not a CORA request has been made — the duty of non-disclosure applies in all contexts.

Category	Examples	Legal Basis / Authority
Executive session content	Discussions, deliberations, and decisions from any executive session; written summaries; identities of persons discussed; legal strategies and advice presented in executive session	C.R.S. § 24-6-402(2)(d.5); BAM § 3.4; BAM § 2.3.3
Personnel records and investigations	Individual performance evaluations, disciplinary records, complaints under investigation, personnel files, medical fitness-for-duty records, compensation details	C.R.S. § 24-72-204(3)(a)(II); BAM § 7.2.2; Policy 200-2.13
Patient and EMS records	Pre-hospital patient care reports, patient identity, medical history, treatment provided, transported to, and any protected health information	HIPAA 45 C.F.R. §§ 160, 164; C.R.S. § 25-3.5-101
Attorney-client communications	All communications between the Board, District Chief, or staff and District Counsel; legal opinions, advice, and strategy; litigation holds; settlement discussions	Attorney-client privilege; C.R.S. § 24-72-204(3)(a)(IV)
Pre-decisional and deliberative records	Draft policies not yet adopted; internal memoranda and working documents not retained in ordinary course; preliminary budget proposals; negotiation positions before Board vote	C.R.S. § 24-72-202(6)(b); CORA deliberative process protection
Security-sensitive information	Station access codes, alarm systems, security camera locations and coverage, apparatus deployment patterns, vulnerability assessments, emergency contact information for critical infrastructure	C.R.S. § 24-72-204(2)(a)(VIII)
Active investigations and incidents	Ongoing personnel investigations; active wildfire or incident investigations where disclosure would compromise public safety; names of complainants who have requested anonymity	Policy 200-2.13 § 4; C.R.S. § 24-72-204(2)(a)(I)
Proprietary third-party information	Vendor pricing submitted in competitive bids; contractor proposals under negotiation; trade secrets in submitted vendor materials; personal financial information of individuals	C.R.S. § 24-72-204(3)(a)(III)-(IV); BAM § 8.1.2
Financial information before adoption	Proposed budgets not yet presented to the Board; preliminary financial projections; grant application strategies; pre-decisional financial analyses	BAM § 6.1; CORA deliberative process protection
Board-designated confidential	Any information specifically designated as confidential by the Board by majority vote or by the Board Chair pursuant to statutory authority	BAM § 2.3.3

What is NOT confidential: Adopted policies and resolutions; approved Board minutes; posted meeting agendas; the District’s annual budget once adopted; general operational procedures in effect; the existence of a public meeting; contact information for the District itself. When a person is uncertain whether information is confidential, they should treat it as confidential and consult the Board Chair (for Directors) or the District Chief (for staff and volunteers) before sharing.

5. THE DUTY OF NON-DISCLOSURE

- a. General prohibition. No person subject to this policy shall disclose, use, publish, discuss, reproduce, or permit access to confidential information except through an authorized disclosure as defined in § 3.



This prohibition applies regardless of whether the person was directly involved in the matter to which the information relates.

b. The need-to-know principle. Confidential information shall be shared within the District only with persons who have a need to know it for a specific District function. The fact that a person is a Director, a senior staff member, or a long-tenured volunteer does not automatically establish need to know for all categories of confidential information. Personnel files, for example, are accessible to the District Chief and Secretary/Treasurer for legitimate employment purposes — not to all Directors or all volunteers simply by virtue of their roles.

c. Deliberative confidentiality. The Board's deliberative process is protected. Board members shall not disclose the substance of deliberations, tentative positions, or preliminary votes from any Board discussion — including work sessions and informal discussions among a quorum — before a final public decision is made. This protection supports the Board's ability to deliberate frankly without external interference, misinformation, or premature community reaction.

d. No use for personal benefit. Confidential information obtained through District service may not be used for personal financial gain, personal advantage, or to benefit any third party. This prohibition applies during and after service. See also Policy 200-2.02 § 10 (Post-Service Obligations) and C.R.S. § 24-18-109 (Colorado Government Ethics Act).

e. Director-specific obligations. Directors are bound by this policy and additionally by BAM § 2.3.3, which establishes the fiduciary dimension of the Director confidentiality obligation. Unauthorized disclosure of confidential information by a Director may constitute a breach of the duty of loyalty as well as a violation of this policy. BAM § 2.3.3 controls in the event of any conflict with this section.

6. OPERATIVE RULES FOR PROTECTING CONFIDENTIAL INFORMATION

The following rules govern how confidential information is handled in daily practice. They apply to all persons subject to this policy in proportion to their access to confidential information and their role in District operations.

a. Conversations and oral communications. Conversations involving confidential information shall not take place in public settings — including restaurants, stores, social events, and any location where the conversation could be overheard by persons not authorized to receive the information. This applies to in-person conversations, telephone calls, and radio communications. Incident scene communications involving patient information, personnel matters, or security-sensitive information shall be conducted through secure channels when practicable.

b. Written and electronic records. Documents, emails, text messages, and other written communications containing confidential information shall be marked or otherwise identified as confidential where practicable. Electronic files shall be stored in password-protected systems or restricted-access locations consistent with Policy 200-2.11 § 6(c). Printed confidential documents shall not be left unattended in common areas, vehicles, or public-facing locations. Physical confidential documents shall be shredded rather than discarded in general waste.

c. Personal devices and personal accounts. Confidential District information shall not be transmitted or stored through personal email accounts, personal cloud storage, or personal social media platforms. Where a Director or personnel member receives confidential District information on a personal device — intentionally or inadvertently — they shall not forward or store that information in third-party applications and shall notify the District Chief or Secretary/Treasurer. Note: messages about District business on personal devices are public records subject to CORA regardless of their confidential content. See Policy 200-2.12 § 5(d).

d. Social media and digital communications. No person shall post, share, publish, or otherwise disclose confidential information through any social media platform, online forum, community group, or digital channel. This includes: executive session content; personnel matters; patient information; pre-decisional draft policies or internal deliberations; active investigation details; security-sensitive information; and any information marked or understood to be confidential. This prohibition applies to all platforms including Facebook, Nextdoor, community email lists, and private messaging applications. See also Policy 200-2.01 § 12 (Social Media and Digital Communications).



- e. Media and public inquiries. Inquiries from the media, members of the public, or other government entities about matters involving confidential information shall be directed to the Board Chair (for governance matters) or the District Chief (for operational matters). No other person shall respond substantively to such inquiries without authorization. Saying “I can’t comment on that” is always appropriate. Saying “I don’t know about that” when the person does know is not required, but the response must not disclose confidential information. See BAM §§ 9.1.1 and 9.1.2.
- f. Authorization to share: the two-step test. Before sharing any information that may be confidential, apply the two-step test: (1) Is this information in one of the ten categories in § 4, or has it been designated confidential by the Board? If yes, go to step 2. (2) Has an authorized disclosure been made for this specific information to this specific recipient? If the answer to both questions is “yes” to the first and “no” to the second, do not share the information. Consult the Board Chair or District Chief first.

7. THE CORA RELATIONSHIP — PUBLIC RECORDS AND CONFIDENTIALITY

The District’s confidentiality obligations and the public’s right of access under the Colorado Open Records Act (CORA) operate on parallel tracks. Understanding the relationship between them is essential for anyone handling District information.

- a. CORA creates a presumption of public access. Colorado law presumes that records created or maintained by government agencies are public records open to inspection. The confidentiality duty in this policy does not override that presumption. When a valid CORA request is received, the records custodian shall respond per the procedures in Policy 200-2.12, including producing records in categories that may otherwise be treated as confidential internally — unless a specific statutory exemption in C.R.S. § 24-72-204 applies.
- b. Confidential information is not always CORA-exempt. The ten categories in § 4 reflect the District’s internal confidentiality obligations. Some of those categories are also CORA-exempt (personnel files, attorney-client communications, executive session materials, patient records). Others may not be. Pre-decisional information, for example, is protected internally but may be subject to CORA once the deliberative process concludes. The records custodian shall consult District Counsel before withholding any category from a CORA response. See Policy 200-2.12 §§ 6(c) and 8.
- c. The duty of confidentiality does not create new CORA exemptions. No one may refuse to produce records in response to a valid CORA request simply because those records are internally treated as confidential. Only a specific statutory exemption in C.R.S. § 24-72-204 justifies withholding. The duty of confidentiality protects against voluntary unauthorized disclosure; it does not authorize CORA non-compliance.
- d. CORA responses and the records custodian. All CORA requests shall be routed to the records custodian (Secretary/Treasurer) on the same day received, per Policy 200-2.12 § 5(b). No person other than the records custodian shall respond substantively to a CORA request. If a CORA request seeks information that appears to the recipient to be confidential, the appropriate response is to route it to the custodian immediately — not to refuse it unilaterally.

Plain statement: The duty of confidentiality governs what you voluntarily share. CORA governs what the District must produce when asked. These are different obligations, managed by different procedures, and neither one overrides the other. When in doubt about a CORA request involving confidential information, route it to the Secretary/Treasurer and consult District Counsel.

8. AUTHORIZED DISCLOSURES

Disclosure of confidential information is authorized in the following circumstances:

- When required by Colorado law, federal law, or court order, including mandatory reporter obligations, CORA responses per Policy 200-2.12, subpoenas, and court-ordered discovery.
- When approved by a majority vote of the Board at a duly noticed public meeting, specifying the information to be disclosed and the recipients or scope of disclosure.
- When made by the District Chief to operational personnel who have a need to know for a specific operational function, consistent with applicable law (e.g., HIPAA for patient records).



- When made by the Board Chair to individual Directors for the purpose of Board deliberation on a specific governance matter, on a need-to-know basis.
- When made to District Counsel for purposes of obtaining legal advice.
- When the information has lawfully entered the public domain through an independent source and no confidential version of the same information remains protected.
- When the person whose confidentiality interest is at stake (e.g., a patient, a personnel subject) gives their informed consent to disclosure in accordance with applicable law.

Note on operational disclosures: The District Chief may authorize sharing of otherwise-confidential operational information (such as incident details, patient information, or personnel assignments) with mutual aid partners, state agencies, or responding entities when operationally necessary and consistent with applicable law. Such authorizations should be documented when practicable.

9. BREACH — REPORTING AND RESPONSE

- a. Reporting a known or suspected breach.** Any person who knows or has reason to believe that confidential information has been disclosed without authorization shall report it to the District Chief (for operational matters) or the Board Chair (for governance matters) as soon as practicable and in any event within twenty-four (24) hours of becoming aware of the potential breach. Reports may also be submitted through the anonymous complaint process in Policy 200-2.13. Reporting a suspected breach is not an accusation — it is a protective measure. No adverse action shall be taken against a person who makes a good-faith report.
- b. Inadvertent disclosure.** A person who inadvertently discloses confidential information — for example, by sending an email to the wrong recipient, leaving a document in a public location, or mentioning protected information in a conversation overheard by others — shall immediately notify the District Chief or Board Chair. Prompt notification enables containment. Concealment of an inadvertent breach is a separate and more serious violation than the breach itself.
- c. Containment and assessment.** Upon receiving a breach report, the District Chief or Board Chair shall: (i) assess the scope and severity of the disclosure; (ii) take immediate steps to limit further dissemination where possible; (iii) notify District Counsel if the breach may have legal consequences, including HIPAA obligations, litigation risk, or personnel implications; and (iv) determine whether formal investigation and/or notification to affected parties is required by law or by the seriousness of the breach.
- d. Investigation.** Intentional or significant inadvertent breaches shall be investigated per the procedures in Policy 200-2.13 or the applicable personnel policy. Where the breach involves a Director, the investigation shall be conducted by disinterested Board members or District Counsel. The investigating officer shall prepare a written report of findings.
- e. HIPAA-specific breach response.** Any breach of patient protected health information (PHI) under HIPAA requires notification to the affected individual and may require notification to the U.S. Department of Health and Human Services (HHS), depending on the scope. HIPAA breach notification requirements are separate from this policy's internal breach reporting requirements and are governed by 45 C.F.R. § 164.400 et seq. The District Chief shall consult District Counsel immediately upon becoming aware of any potential HIPAA breach.

10. ENFORCEMENT AND CONSEQUENCES

Violations of this policy are subject to the enforcement procedures in Policy 200-2.01 § 7 and the progressive discipline procedures in Policy 300-3.13 (pending). Consequences shall be proportionate to the severity of the violation and may include:

- For paid staff and volunteers: counseling, written warning, suspension, or termination consistent with Policy 300-3.13;
- For Directors: formal written censure by Board resolution at a duly noticed public meeting; mandatory additional ethics and confidentiality training; referral to the Colorado Independent Ethics Commission; or referral to law enforcement where criminal conduct is alleged;



- For contractors: contract suspension or termination and disqualification from future District engagement;
- For all persons: civil liability if the breach causes compensable harm to an identifiable person (e.g., disclosure of patient records, disclosure of personnel information).

No adverse action shall be taken against any person for making a good-faith report of a breach or suspected breach, for participating in a breach investigation, or for declining to disclose confidential information in accordance with this policy.

11. ACKNOWLEDGMENT AND TRAINING

- Annual acknowledgment. All Directors, paid staff, and active volunteers shall review this policy upon joining the District and annually thereafter, and shall sign the Annual Code of Ethics Acknowledgment Form (Policy 200-2.01, Appendix A), which encompasses acknowledgment of the confidentiality obligations in this policy. A separate standalone acknowledgment form is not required; the Policy 200-2.01 form serves both purposes when the person has reviewed this policy.
- Training. Confidentiality training shall be incorporated into the annual ethics training cycle per Policy 200-2.01 § 9. Training shall specifically cover: the ten categories in § 4; the social media prohibitions in § 6(d); the CORA relationship explained in § 7; and the breach reporting obligation in § 9. For Directors, confidentiality training shall be incorporated into the OML training required by Policy 200-2.07 § 10.
- Contractors. Contractors and vendors who are granted access to confidential information shall receive a summary of this policy’s key obligations — at minimum, the categories in § 4 and the prohibition in § 5 — before that access is granted.

12. ANNUAL REVIEW AND AMENDMENT

This policy shall be reviewed in the Q1 annual review cycle per Policy 100-1.06. The District Chief shall identify any changes in Colorado law affecting confidentiality obligations — particularly amendments to CORA exemptions, HIPAA regulations, or the Colorado Government Ethics Act — and present them to the Board as proposed amendments at the Q1 annual review meeting. The District Chief does not update the policy text; any amendment requires Board approval per Policy 100-1.06 § 5. Amendment requires a majority Board vote per Policy 100-1.06 § 5.

13. SEVERABILITY

If any provision of this policy is held invalid or unenforceable, the remaining provisions shall continue in full force and effect.

PASSAGE AND ADOPTION.

PASSED, APPROVED, AND ADOPTED by the Board of Directors of the Southern Park County Fire Protection District at a duly noticed public meeting, by the following vote:

Director	AYE	NAY	ABSTAIN
Sean English (Board Chair)	AYE		
Mike Brandt (Secretary/Treasurer)	AYE		
Mike Parrish	AYE		
Mike Smith	☐		
Jennifer Taylor	AYE		



ATTESTATION.

IN WITNESS WHEREOF, the undersigned duly authorized officers hereby attest to the adoption of this policy.

Sean English

Board Chair — Board of Directors, SPCFPD

Date: May 12, 2026

Mike Brandt

Secretary/Treasurer — Board of Directors, SPCFPD

Date: May 12, 2026

Mike Parrish

Board Member — Board of Directors, SPCFPD

Date: May 12, 2026

Mike Smith

Board Member — Board of Directors, SPCFPD

Date: _____

Jennifer Taylor

Board Member — Board of Directors, SPCFPD

Date: May 12, 2026

CERTIFICATION.

I, Mike Brandt, Secretary/Treasurer of the Board of Directors of the Southern Park County Fire Protection District, Park County, Colorado, hereby certify that the foregoing is a true and correct copy of Policy 200-2.04 duly adopted by the Board of Directors at a duly noticed public meeting, at which a quorum was present and acting throughout.

Mike Brandt

Secretary/Treasurer — Southern Park County Fire Protection District

Date: May 12, 2026



Document Revision History

Document: 20260408_ADMIN_200-2.04_ConfidentialityNonDisclosure_DRAFT-v0.4 Policy: 200-2.04 — CONFIDENTIALITY AND NON-DISCLOSURE

Table with 4 columns: Ver., Date, Author, Changes / Status. Rows include v0.1 through v1.0, detailing revisions such as 'Initial adoption', 'Amendment 9 of 10', 'BAM version reference update', and 'Formally adopted at regular board meeting'.

This policy shall be interpreted consistently with: BAM v0.8 (§§ 2.3.3, 9.1.3); Policy 100-1.02 (Mission, Core Values & Ethics §§ 5.3, 5.7); Policy 200-2.01 (Code of Ethics and Conduct §§ 5, 12); Policy 200-2.12 (CORA Compliance Procedure); Policy 200-2.11 (Records Retention Schedule and Procedures); Policy 200-2.13 (Citizen Complaint Procedure); Policy 300-3.13 (Progressive Discipline — pending); C.R.S. § 24-6-402(2)(d.5) (Executive Session Recordings); C.R.S. § 24-72-201 et seq. (CORA); HIPAA 45 C.F.R. Parts 160 and 164; C.R.S. § 24-18-101 et seq. (Colorado Government Ethics Act); C.R.S. § 25-3.5-101 et seq. (EMS and Patient Records).

— END OF POLICY 200-2.04 —