CITY OF FLAGSTAFF

PRESENTATION TO CITY COUNCIL

Technology Privacy Review Process

Privacy principles and the review process for new technology and renewals

November 10, 2026 · CJ Perry · Chief Information Officer

Agenda

From where the Task Force has been to the update staff is bringing to Council today

1. Privacy Task Force Timeline
2. Overview of City IT
3. Existing and Draft Processes
4. Review of Privacy Principles
5. Review of Process for New Technology and Renewals
6. Next Steps
7. **Council Questions and Input**

Privacy Task Force Timeline

How we got here, and where the work goes next

Mar. 16, 2026

Task Force formed

Charge, membership and first meeting

May 18, 2026

Privacy principles drafted

Drafting and review meetings

Sep. 21, 2026

Review process developed

Directive, screening questions and report form

Oct. 19, 2026

Task Force input

Reviewed the principles and process and provided input to staff

Today

City Council presentation

Staff presents this process and outline to Council for awareness

Overview of City IT

The people and systems behind City service delivery

18 Divisions
67 Sections
51 Programs
1,000+ Employees
77,000+ Residents

Depend on the divisions for reliable, efficient and streamlined processes and systems that create high uptimes and high-quality service delivery.

1,160 Users supported	**1,272** PCs and laptops	**731** Mobile devices
26 Physical Servers **146** Virtual Machines	**76** Primary Applications	**45** City connected sites
134 Wireless access points	**250+** Public safety radios	**200,000+** GIS mapped assets

Every Interaction Creates Data

Resident services and internal operations both generate information the City must protect

From Residents

- Summer camp sign-ups at the Aquaplex
- Water, sewer and trash service accounts
- Business licenses at the front counter
- 911 calls and Fire medical records
- Contractor permit applications
- Traffic citations and body-worn camera footage
- Senior classes at Joe C. Montoya
- Library cards

Inside the City

- Sales tax analysis and building permit reports
- Council communications and recommended contracts
- Procurement and RFP records
- Employment history and recruitments
- Policies, directives and City financials
- Emergency management and preparedness plans
- Housing, energy and sustainability metrics
- Water meters and forest stormwater gauges

All of these interactions and systems create data. We work with organizational partners to protect it.

EXISTING AND DRAFT PROCESSES

How is City data managed, and where is it stored?

On-premises and hosted solutions are governed by laws, regulations, and local directives.

CITY OF FLAGSTAFF

Data and Privacy Framework

City data lives in on-premises and hosted solutions; its use, storage and retention are governed at every level

Governed by Laws, Regulations & Standards

State statute
Records retention schedules (A.R.S. § 39-121), data breach notification laws (A.R.S. § 18-551, 18-552) and more

HIPAA
Federal and state health information privacy laws

CJIS
Criminal Justice Information Services security policy and state law (e.g., A.R.S. §41-1750, 41-1959, 41-619.54)

Other state and federal regulations

Best practices and industry standards
Such as NIST and CISA

Local governance framework and directives

Local Structure for Data Use

Cybersecurity requirements
Army National Guard Audits
Department of Homeland Security Audits
Multiple minor audits throughout the year

Data classifications
Define the types of data and their use:
- Public
- Internal
- Confidential
- Restricted

Other Technology Related Directives
Multiple City Manager Directives
Multiple Division Level Directives

City Manager Directives

Three directives set clear expectations for how employees use City systems, tools and data

DIRECTIVE
Acceptable Use

Outlines expectations for use of City business systems and applications

- Provides for periodic audits and reviews of logs
- Allows review of files and activity as needed, through an approval process
- Designed for clarity and accountability
- Rolling out for signature this fall

DIRECTIVE
Artificial Intelligence

Outlines expectations for the use of AI tools

- Defines what data can and cannot be shared with AI tools
- Defines what AI tools can and cannot be used

DIRECTIVE
Technology Privacy

Articulates how the City evaluates technology for privacy

- Core privacy principles
- The process new technology and renewals will follow
- Expectations for technologies staff may wish to introduce into the environment

Division Directives & Procedures

There are multiple other Directives and Procedures already in place

PROCEDURE

Management Services

Management Services manages all contracts and procurements:

- Procurement Manual

Typical reviews during this process:

- Legal Review
- IT Review

https://www.flagstaff.az.gov/2991/Procurement-Code-Manual

DIRECTIVE

Police Department

The Police Department Operations Orders cover a wide range of procedures including:

- Information Technology Use
- Drone / Unmanned Aerial Systems Operations
- Mobile Audio Video (body-worn camera)
- Training… Accountability… Officer Wellness… Operations

https://www.flagstaff.az.gov/2736/Forms-Operations-Orders

PROCEDURE

Public Process

City Council acts as the final approval via a public process:

- Agenda Review
- Public Comment
- Elected Approval
- Public Records Requests

https://www.flagstaff.az.gov/991/Agendas-Minutes

Cybersecurity Practices

Other layers of protection behind every technology the City adopts

Privacy task force review is one layer of many.

Our cybersecurity practices protect City systems and the data they hold, working alongside the privacy review process.

STATE GUIDANCE

AZ Department of Homeland Security

We follow AZDOHS cybersecurity best practices.

INDEPENDENT AUDITS

Army National Guard Cyber Division

We perform security audits with the Army National Guard Cyber Division.

NATIONAL FRAMEWORK

NIST Cybersecurity Framework

We judge ourselves against the NIST Cybersecurity Framework and related best practices.

CONTRACT REVIEW

Application Contract Checklist

Every software contract is reviewed to ensure the City is protected.

Together, these directives and processes provide a coordinated wrap around our data, systems and organizational expectations.

No one directive sets the stage; they work together in harmony to collectively address data governance and privacy.



Privacy Principles

All City activities involving the collection and use of data shall be guided by the following principles (summarized)

1 Necessity and Proportionality
The City uses technology and data only to achieve specific, legitimate public purposes and governmental operations.

2 Transparency and Community Engagement
To the extent possible, the public has a right to know what we collect, why, and how it is used. We consider public perspectives, including through the Task Force.

3 Use Limitation
Technology and data are used in compliance with law, and never used or shared for personal use or commercial purposes.

4 Data Security
Administrative, technical and physical safeguards protect technology and data from unauthorized access, use, destruction or disclosure.

5 Accountability
Governance, training and auditing hold the City accountable, with logs and audit trails scaled to data sensitivity and risk.

6 Data Sharing
Sharing technology and data must serve governmental services, with appropriate protections, legal compliance and documentation.

7 Data Retention
Data is kept only as long as needed for its purpose or required by law and retention schedules, and may be kept for historical reference.

8 Privacy by Design
Where feasible, privacy protections, data minimization and de-identified data are built into how systems are designed and deployed.

Phase 1 · Division Input

EXISTING PROCESS

Every review starts the way it always has: with the requesting division

PRIVACY PRINCIPLES govern every phase

1 Division Input	2 City Manager Directive	3 Privacy Task Force Meeting	4 Procurement or Contracts	5 City Council Consideration

Owner: Requesting Division

Procurement		Contract Renewal
A new solicitation or RFP for technology the City wants to acquire	*OR*	A renewal of a technology contract the City already has in place

The requesting division starts the process with a new solicitation or a renewal. Nothing about this starting point is new.

NEXT · PHASE 2



Every request now passes through the City Manager Directive screening

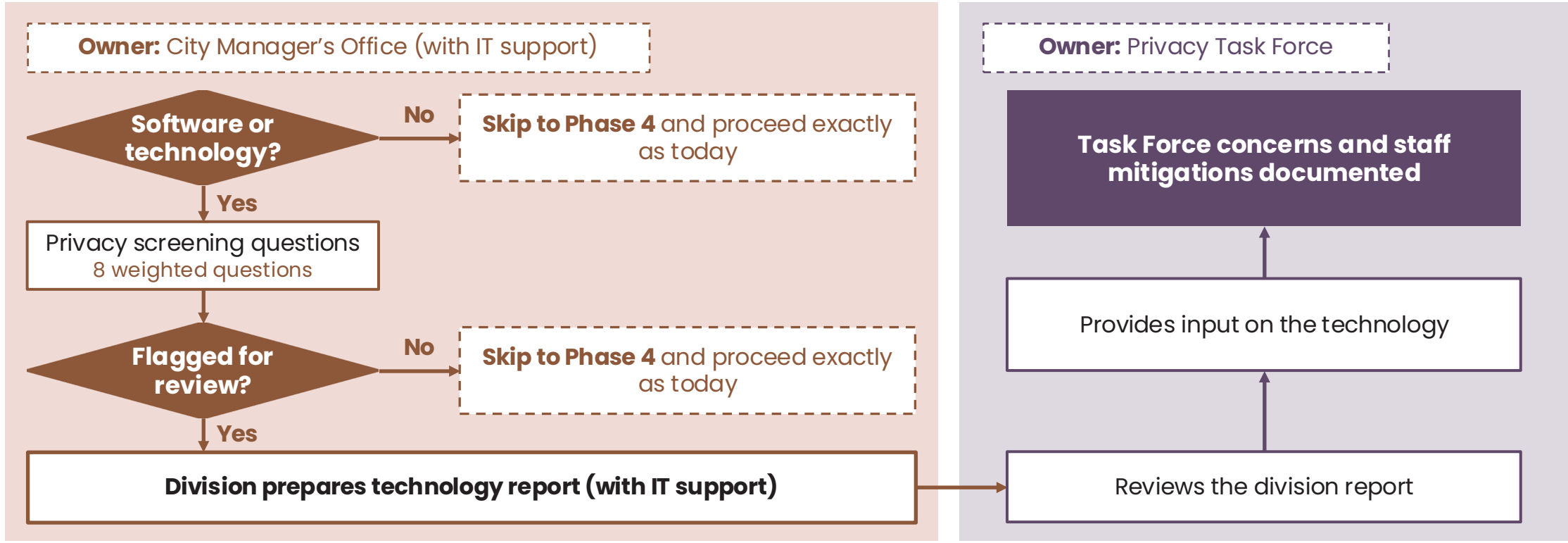
Phases 2 & 3 · What's New

NEW TO THE PROCESS

A quick screening sorts technology, and only flagged items go to the Privacy Task Force

PRIVACY PRINCIPLES govern every phase

1 Division Input | **2 City Manager Directive** | **3 Privacy Task Force Meeting** | 4 Procurement or Contracts | 5 City Council Consideration



Phases 4 & 5 · Existing Process

EXISTING PROCESS

Procurement and Council approval continue as they do today, now with Task Force input attached

PRIVACY PRINCIPLES govern every phase

1 Division Input | 2 City Manager Directive | 3 Privacy Task Force Meeting | **4 Procurement or Contracts** | **5 City Council Consideration**

Owner: Procurement / Contracts

RFP process or contract negotiation continues

- **Legal Review**
- **IT Security Review**

Items not flagged in Phase 2 arrive here directly and proceed exactly as they do today.

IT's security review asks objective questions (data ownership, AI training, encryption, compliance, access control). Answers never flag an item for the Task Force.

Owner: City Council

Task Force notes and staff mitigation efforts appended to report

Submitted to City Council

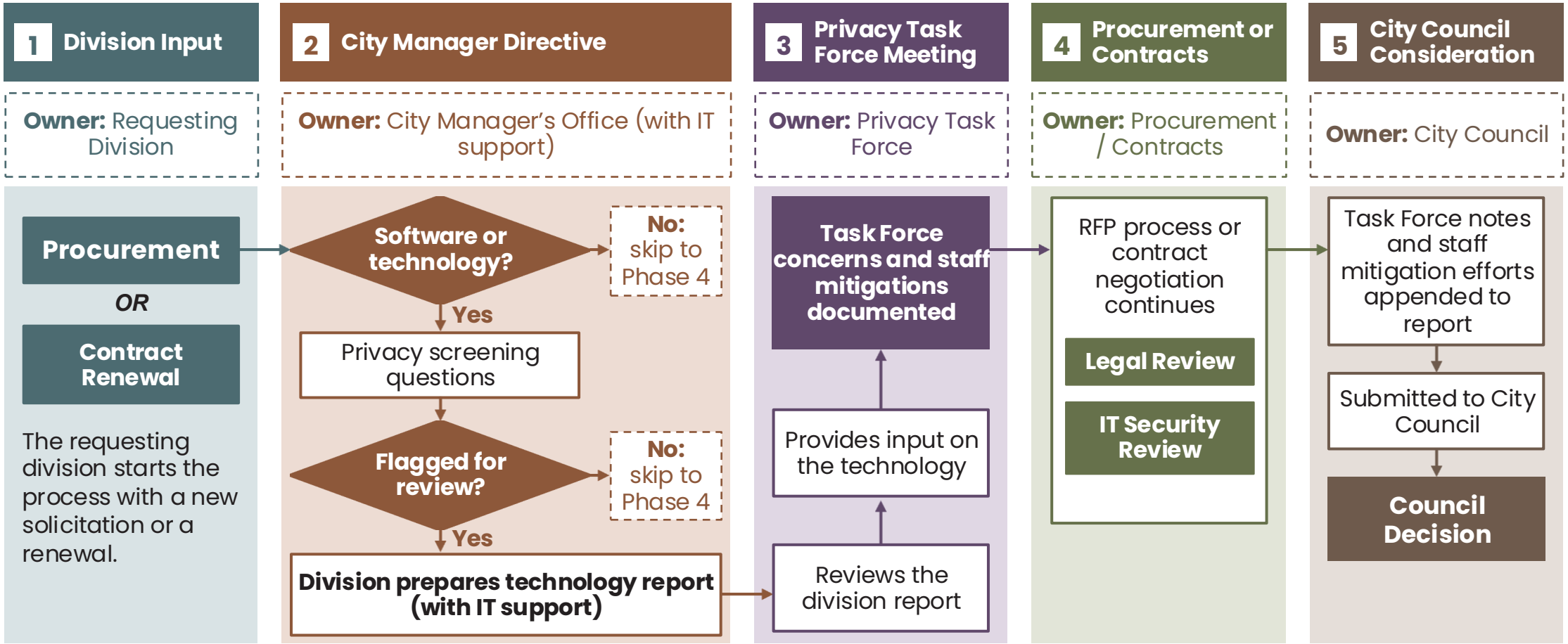
Council Decision

Agenda review · Public comment · Elected approval

Technology Privacy Review Process

From RFP or contract renewal to City Council approval, and who owns each phase

PRIVACY PRINCIPLES govern every phase



Privacy Screening Questions

Asked in Phase 2 under the City Manager Directive to gauge privacy concerns

QUESTION 1 · DATA TYPE
What type of data is collected?

1	No personal data
2	Basic contact data
3	Legally protected PII
4	Incidental point in time data
5	Ongoing general capture

QUESTION 2 · DATA SHARING
How is this data shared with other agencies?

1	No sharing capabilities at all
2	Sharing managed under existing policy or directive
3	General to other agencies without City request

Answer key Low weight · Medium weight · Heavy weight · Offsetting weight

Privacy Screening Questions

Asked in Phase 2 under the City Manager Directive to gauge privacy concerns

QUESTION 3 · RETENTION
How long is identifiable data kept?

1	Not captured
2	Retention period set by law
3	30 days or less
4	31 to 90 days
5	More than 90 days, or no set limit

QUESTION 4 · NOTICE & CONSENT
Is there a notification (signs, warnings, etc.) or opt-in method for data capture?

1	Not applicable (no data collected)
2	Yes (requires user to volunteer data)
3	Yes (there are signs notifying the public of data collection)
4	No (PII collected without consent or knowledge)

Answer key Low weight · Medium weight · Heavy weight · Offsetting weight

Privacy Screening Questions

Asked in Phase 2 under the City Manager Directive to gauge privacy concerns

QUESTION 5 · CAMERAS ONLY · FOCUS
What is it focused on?

1	Not applicable
2	Land, infrastructure, assets, or the environment
3	Protecting a facility and the people in it
4	Crowds or general public activity during an event
5	Locating, following, or investigating specific people or vehicles

QUESTION 6 · LAW ENFORCEMENT ONLY · USE
Who uses it, and how?

1	Not applicable
2	Non-enforcement data for operations, planning, or maintenance
3	Law enforcement reviews recordings post victimization
4	Law enforcement uses it in real time to locate or investigate suspects

Answer key Low weight · Medium weight · Heavy weight · Offsetting weight

Privacy Screening Questions

Asked in Phase 2 · Green answers offset other weights and may give the technology a pass

QUESTION 7 · ANONYMIZATION
Is data anonymized?

1. **Yes**
2. **No**

QUESTION 8 · DATA ORIGIN
Does the technology create new data or analyze existing data?

1. **Existing data**
2. **New data**

Answer key Low weight · Medium weight · Heavy weight · Offsetting weight

IT Security Review Questions

Asked by IT during its cybersecurity review in Phase 4, separate from the privacy screening

01 DATA OWNERSHIP
Who owns the data?

02 Artificial Intelligence
Does AI train against our data?

03 ENCRYPTION
How is the data encrypted?

04 COMPLIANCE
Which regulatory frameworks apply?

05 ACCESS CONTROL
Does it integrate with existing access controls?



Not part of the privacy review.

IT asks these questions during its security review, alongside Legal Review. Answers do not flag an item for the Privacy Task Force.

Technology Report

Technology Privacy Disclosure Form, prepared in Phase 2 by the department (with IT support) when an item is flagged

Software title
A specific vendor/software name, or a category of software type if still in procurement/selection.

A description of the technology and its proposed use.

The specific purpose(s) the technology will advance.

A detailed description of what data is collected.

A clear statement of what data is not collected.
Data that might be a privacy concern that we are purposefully excluding from collection to ensure privacy.

What are the applicable retention schedules?

What data is likely to be shared with other agencies, organizations or people outside of City staff?
Policy references, the data sharing process, and what and how data is shared.

List any mitigation efforts to protect collected data and the privacy of Flagstaff residents.
Audit controls, automatic data deletion, anonymization, etc.

EXAMPLE TECHNOLOGIES

How do the screening questions work in practice?

Two familiar technologies, with each answer color coded by its weight.

CITY OF FLAGSTAFF

Adobe PDF Reader

Example technology · Software for reading PDFs

Q1 · What type of data is collected?	**No personal data**
Q2 · How is this data shared with other agencies?	**No sharing capabilities at all**
Q3 · How long is identifiable data kept?	**Not captured**
Q4 · Is there a notification (signs, warnings, etc.) or opt-in method for data capture?	**Not applicable (no data collected)**
Q5 · (Cameras only) What is it focused on?	**Not applicable**
Q6 · (Law enforcement only) Who uses it, and how?	**Not applicable**
Q7 · Is data anonymized?	**No**
Q8 · Does the technology create new data or analyze existing data?	**Existing data**

Answer key Low weight · Medium weight · Heavy weight · Offsetting weight

Public Facing Security Cameras

Example technology · Security cameras at City facilities that can observe parking lots and public spaces

Q1 · What type of data is collected?	Ongoing general capture
Q2 · How is this data shared with other agencies?	Sharing managed under existing policy or directive
Q3 · How long is identifiable data kept?	30 days or less
Q4 · Is there a notification (signs, warnings, etc.) or opt-in method for data capture?	No (PII collected without consent or knowledge)
Q5 · (Cameras only) What is it focused on?	Crowds or general public activity during an event
Q6 · (Law enforcement only) Who uses it, and how?	Law enforcement reviews recordings post victimization
Q7 · Is data anonymized?	No
Q8 · Does the technology create new data or analyze existing data?	New data

Answer key Low weight · Medium weight · Heavy weight · Offsetting weight

Next Steps

What happens after today's Council update

1

AFTER EACH REVIEW

Task Force input travels with the contract

After Task Force discussion, the memo and any mitigations are included in the staff summary for Council with any proposed contract.

2

TODAY

Council briefed on the process

Flagged items will reach Council with Task Force input and staff mitigations attached.

3

ONGOING

Keep improving

We will continue to modify and iterate on these directives and this process as we find opportunities to improve.

It is important to get these guardrails in place sooner rather than later.

CITY OF
FLAGSTAFF

Questions?

Thank you to the Citizen Privacy Task Force for its work.

CJ Perry · Chief Information Officer