ChatGPT

Privacy Governance in APS: Impactful Actions (STAR Examples)

In the Australian Public Service (APS), strong privacy governance is essential, especially for roles handling sensitive information like a Freedom of Information (FOI) Practice Manager in the Department of Home Affairs. Working in compliance with the APS Code of Conduct means adhering to legal requirements and upholding confidentiality. The APS Code explicitly requires employees to **comply with all applicable Australian laws** (such as the Privacy Act 1988 and FOI Act 1982) and to **maintain appropriate confidentiality of official information** [1] [2]. The Department's privacy policy implements these obligations by following the Privacy Act's 13 Australian Privacy Principles (APPs), which regulate the **collection, use, disclosure, and storage of personal information** [3]. In practice, some of the most impactful privacy governance actions include:

- **Strict compliance with privacy laws and policies:** Ensuring all handling of personal data aligns with the Privacy Act, APPs, and the Department's privacy policy (no unauthorized use or disclosure of personal information).
- **Safeguarding personal information:** Securing records (digital and physical) so that only authorized personnel can access them and using information only for its official purpose [4]. This includes applying the Protective Security Policy Framework (PSPF) guidelines, such as classifying sensitive data and enforcing "need-to-know" access controls.
- **Balancing FOI transparency with privacy:** Applying FOI Act provisions to protect individual privacy (e.g. using the personal information exemption when appropriate) while still facilitating access to information. In other words, release what you can, **redact what you must** to prevent unreasonable disclosure of others' personal details [5].
- **Proper retention and disposal of data:** Keeping personal information only as long as required and then **securely destroying or archiving it** in line with records authorities and the Archives Act [6]. This prevents accumulation of unnecessary personal data and reduces privacy risk.

Below are two STAR examples demonstrating how an EL1 FOI Practice Manager might embody these actions, showing impactful privacy governance in line with APS values and the Department's privacy policy.

Example 1: Safeguarding Personal Information in an FOI Release (STAR)

Situation: In her role as an FOI Practice Manager, Jane (EL1) received a complex FOI request seeking documents related to a program audit. Some of the responsive documents contained **personal information about third parties** (e.g. names and contact details of individuals who were mentioned in internal emails). Releasing everything as-is would risk **exposing private details**, potentially breaching the Privacy Act and departmental policy. This put Jane in a position of balancing the FOI Act's transparency objective with the **privacy rights** of individuals.

Task: Jane's task was to process the FOI request in accordance with the law and policy – meaning she needed to **give the applicant maximum access to information** while **protecting any personal or sensitive data** that should not be disclosed. She had to identify which parts of the documents were

exempt from release on privacy grounds, justify those redactions under the FOI Act, and ensure her actions complied with the Department of Home Affairs Privacy Policy and the APS Code of Conduct. (Under the Privacy Act's APPs, personal data should only be disclosed in ways that are authorized by law [3], and the FOI Act provides a specific exemption for unreasonable disclosures of personal information [5].)

Action: Jane carefully reviewed each document line by line, flagging any content that revealed personal identifiers (such as private addresses, phone numbers, or names of junior staff and members of the public). She consulted **Section 47F of the FOI Act**, which is the *personal privacy exemption*, confirming that disclosure of those details would be an "unreasonable disclosure of personal information" about someone other than the applicant [5]. In accordance with that provision, and guided by the Department's privacy policy, she decided to **redact** (black out) the names and contact details of third parties while **releasing the remaining information**. Jane ensured that any personal information **belonging to the FOI applicant** themselves was left intact, since individuals have the right to access their own personal information (and such information would not be exempt) [7]. To maintain transparency, she documented her reasoning in the decision letter, citing the FOI Act exemption for personal privacy and explaining that those redactions were made to **protect individuals' privacy** in line with departmental policy. Before finalizing, Jane double-checked that all redactions were necessary and consulted the Department's Privacy Officer for a quick review of the sensitive excerpts, showing due diligence in privacy governance. She also verified that the **redacted documents were properly marked** (e.g. "Edited Copy – s47F redactions") and that no metadata or hidden personal data remained in the electronic files.

Result: Jane released the FOI documents to the applicant on time, with clear markings where information had been redacted to protect third-party privacy. The applicant received all the substantive information they sought, minus the personal identifiers of other people. There were **no complaints or internal review requests** about the handling of personal information – in fact, by preemptively addressing privacy concerns, Jane prevented potential privacy breaches or complaints to the Office of the Australian Information Commissioner. The outcome upheld **both** open government principles and the Privacy Act obligations, exemplifying how to lawfully balance transparency with privacy. This successful FOI release reinforced that Jane **acts with integrity and diligence**, as expected of an APS employee, and strictly follows the Department's Privacy Policy. Her actions in this situation were directly **in accordance with the Australian Privacy Principles and departmental privacy rules** on disclosure of personal data [3], as well as the APS Code of Conduct requirement to comply with law and protect confidential information. This example demonstrates an impactful privacy governance action: using legal exemptions and privacy principles to **prevent unauthorized personal information disclosure while delivering services**.

Example 2: Protecting Candidate Data in Recruitment Processes (STAR)

Situation: In addition to FOI duties, Jane also manages recruitment of legal support staff in her division. Recently, she led a hiring round for new legal officers. This process involved handling **sensitive personal information** from dozens of applicants – including resumes with personal details, academic records, and background check results (some candidates provided copies of IDs and security clearance confirmations). All this information was provided in confidence for recruitment purposes. The situation posed a significant privacy governance challenge: **how to collect, use, and store applicant data responsibly** so that the Department meets its privacy obligations and candidates' information is kept safe from improper access or disclosure.

Task: Jane's task was to run a fair and efficient recruitment while **ensuring the personal information of applicants was protected at every stage**. Practically, this meant she had to limit access to these documents, secure both electronic and hard copy records, and ultimately dispose of or retain them properly after the process. She also needed to make sure **everyone involved in the hiring panel respected confidentiality**. Her goal was to comply with all relevant policies – the Department's Privacy Policy, APS Code of Conduct, and Australian Privacy Principles – which require using personal data **only for the intended purpose and keeping it confidential** [4]. She also had to adhere to government record-keeping rules for any documents kept on file, such as applications from successful candidates.

Action: Jane implemented several concrete privacy safeguards during the recruitment. First, she **collected only the information needed** for assessing candidates (for example, she did not ask for unnecessary personal details). On receiving applications, she ensured they were stored on a **secure internal system** with access restricted to the HR team and the selection panel members **on a need-to-know basis** [4]. Electronic files were saved in a folder with permissions set only for the panel, and physical documents were kept in a **locked cabinet** in her office. She reminded the panel members of their **confidentiality obligations** under the APS Code of Conduct (e.g. not to discuss candidate details outside the panel). During shortlisting and interviews, Jane marked printed materials as "OFFICIAL: Sensitive" since they contained personal particulars, aligning with the Protective Security Policy Framework guidance on classifying information.

After the recruitment was completed, Jane took care to **dispose of personal data securely**. For candidates who were not hired, she followed the Department's records management policies: **shredding** or pulping paper files of resumes and forms, and deleting digital files from the shared drive after the required retention period. (According to government privacy guidelines, when personal information is no longer required, it should be **destroyed in a secure manner** to prevent any further disclosure [6].) For the successful candidate, she transferred the necessary personal documents into the Department's HR system and ensured any extra copies were destroyed. By doing this, Jane made sure that personal information **was not kept longer than needed** and that it couldn't be accessed by anyone once the process was over. Throughout the recruitment, she also handled any queries from applicants about privacy by referring them to the Department's Privacy Policy notice (which was included in the job application pack), showing transparency about how their data would be used.

Result: The recruitment process concluded with **no privacy incidents** – there were no lost documents, no unauthorized access, and no complaints from applicants about misuse of their information. All panel members strictly followed the protocols Jane set, which meant applicant data remained confidential and was used **only for its intended purpose (the hiring decision)** [4]. By promptly and securely disposing of the personal data of unsuccessful candidates, she eliminated the risk of that data being mishandled in the future, in line with best practices and the department's privacy guidelines. Jane's diligent privacy governance had a positive impact on team culture as well: her staff gained a stronger awareness of privacy requirements, seeing them modeled in action. This example highlighted Jane's commitment to **accountability and respect** (APS Values) – she treated candidates' personal information with the utmost care and **ensured compliance with all relevant policies**. Her actions mirrored the department's Privacy Policy commitments to secure storage and proper handling of personal information, as well as the APS Code of Conduct's standards for confidentiality and lawful conduct. Overall, this experience proved Jane to be a trustworthy custodian of sensitive data, an attribute highly valuable for an EL2 role.

Conclusion

In summary, **the most impactful privacy governance actions** for an APS employee in Jane's position are those that **embed privacy compliance into everyday work**. By strictly adhering to privacy laws and the Department of Home Affairs' Privacy Policy, securing personal data against unauthorized access, exercising judgment to **withhold private information when releasing documents**, and responsibly managing the information lifecycle (from collection to destruction), she not only upholds the APS Code of Conduct but also fosters public trust. These examples illustrate how applying the APS values of integrity, accountability, and respect in practical situations – through the STAR framework – leads to outcomes that are both **helpful (protecting individuals' privacy)** and **useful (ensuring departmental compliance and reputation)**. Jane's demonstrated actions in privacy governance show she is prepared to take on the higher responsibilities of an EL2 role, continuing to champion privacy and confidentiality as integral parts of public service excellence.

Sources:

1. Australian Public Service Commission – *APS Code of Conduct* [8] (Legal compliance and confidentiality requirements for APS employees)
2. Department of Home Affairs – *Privacy Policy Summary* [3] (Obligations under the Privacy Act and APPs)
3. Department of Home Affairs – *Privacy (Access and Correction)* [7] (Individuals' right to access their own information under Privacy/FOI laws)
4. Freedom of Information Act 1982 – *Section 47F (Personal Privacy Exemption)* [5] (Basis for redacting personal info in FOI releases)
5. Department of Home Affairs – *Web Privacy Statement (Security of Information)* [4] (Protective Security Policy Framework – only authorized access, official purpose use)
6. National Emergency Management Agency – *Privacy Policy* [6] (Secure destruction of personal information when no longer required)

---

[1] [2] [8] APS Code of Conduct | Australian Public Service Commission
https://www.apsc.gov.au/working-aps/integrity/integrity-resources/code-of-conduct

[3] [6] Privacy and disclosures | NEMA
https://www.nema.gov.au/about-us/privacy-disclosures

[4] Web privacy
https://www.homeaffairs.gov.au/access-and-accountability/using-our-website/web-privacy

[5] Section 47F – Personal Privacy Exemption
https://www.auxlaw.com.au/insights/section-47f-personal-privacy-exemption

[7] Privacy
https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/privacy