

Code of Ethics and Conduct

Policy Number:	POL22/40	Version:	1.1
Authorised by:	Gary Barnes, Secretary DRNSW	Authorised date:	May 2020
Issued by:	Legal and Governance	Effective date:	1 July 2020
		Review date:	1 July 2022

© State of New South Wales through Department of Regional NSW 2020. You may copy, distribute, display, download and otherwise freely deal with this publication for any purpose, provided that you attribute the Department of Regional NSW as the owner. However, you must obtain permission if you wish to charge others for access to the publication (other than at cost); include the publication in advertising or a product for sale; modify the publication; or republish the publication on a website. You may freely link to the publication on the departmental website.

Disclaimer: The information contained in this publication is based on knowledge and understanding at the time of writing in May 2020 and may not be accurate, current, or complete. The State of New South Wales (including the NSW Department of Regional NSW), the author and the publisher take no responsibility, and will accept no liability, for the accuracy, currency, reliability, or correctness of any information included in the document (including material provided by third parties). Readers should make their own inquiries and rely on their own advice when making decisions related to material contained in this publication.

The Department of Regional NSW acknowledges that it stands on Country - always was and always will be Aboriginal land. We acknowledge the Traditional Custodians of the land and waters, and we show our respect for elders past, present and emerging.

We are committed to providing places in which Aboriginal people are included socially, culturally, and economically through thoughtful and collaborative approaches to our work.

Contents

Introduction and application of the Code	3
Standards of conduct.....	4
Professional standards.....	5
Work health and safety.....	6
Respect and inclusion.....	6
Managing conflict of interests.....	8
Conflict of duty.....	9
Senior executive private interests.....	9
Employment outside the department	9
Gifts, benefits, and hospitality	9
Flexible workforce	10
Leaving the department	10
Departmental resources	11
Appropriate use of resources	11
Budget.....	11
Buying goods and services.....	12
Intellectual property and copyright.....	13
Managing grant and funding agreements	13
Managing information.....	14
Records management.....	14
Confidentiality and privacy	14
Requests for information.....	15
Cyber security	16
Making good decisions	17
Complying with legislation and policy.....	17
Risk management.....	18
Business improvement – audits, inquiries, and investigations	18
Engaging with the community	20
Stakeholder engagement.....	20
Lobbyists	20
Managing complaints about the services we provide	20
Sponsorships	21
Speaking up and reporting matters	22
Confidential reporting options and requirements.....	22
Fraud, corruption, and maladministration.....	23
Criminal offences and bankruptcy	24
Breach of the Code.....	25
Computer and other workplace surveillance.....	25
How to contact our subject matter experts.....	26

Introduction and application of the Code

The Department of Regional NSW (the department) Code of Ethics and Conduct (the Code) sets out the standards of behaviour expected of all departmental employees. To make it easier for people to understand their responsibilities, this Code links to extra information and procedures where required. It also links directly to supporting systems, where these are available.

Our department is diverse. Some areas may have specific ethics and conduct requirements related to their specific functions. For example: regulators may have stricter requirements for gifts and benefits. Funding or procurement bodies may have stricter requirements for conflict of interests. It is important that you take the time to understand not only the responsibilities that apply to all employees, but also any extra responsibilities that may apply in your area. Resources Regulator staff refer to the Regulator's Integrity Framework and Integrity Clearance policy.

This Code applies to all employees of the department. It also applies to volunteers, contingent workers, independent contractors, and consultants engaged by the department, except for those aspects such as performance and development plans that are only applicable to employees.

If you are a member of a board or committee and hold that position as a nominee of the Secretary or Minister (that is, you are there in your capacity as an officer of the department), the department Code applies. A board or committee may have its own code of conduct or rely on the [NSW Government Boards and Committees Guidelines](#). In that case, you will have obligations under both this Code and the committee or board code.

Many of the responsibilities in this Code apply to all employees. In some instances, senior executives, people leaders or subject matter experts have more responsibilities. For the purposes of this Code, the following definitions apply:

- A **people leader** is anyone who is responsible for managing other people within the department.
- A **subject matter expert** is anyone in a role that has responsibility for a functional area.

Standards of conduct

The department works to the same ethical framework and values as almost 400,000 other public sector employees. The objectives of the framework are to:

- recognise the role of the government sector in preserving the public interest, defending public values, and adding professional quality and value to the commitments of the government of the day
- establish an ethical framework for a merit-based, apolitical, and professional government sector that implements the decisions of the government of the day.

The objectives are supported by the NSW Government sector core values which are set out in the Government Sector Employment Act 2013:

Integrity

- Consider people equally without prejudice or favour
- Act professionally with honesty, consistency, and impartiality
- Take responsibility for situations, showing leadership and courage
- Place the public interest over personal interest.

Trust

- Appreciate difference and welcome learning from others
- Build relationships based on mutual respect
- Uphold the law, institutions of government and democratic principles
- Communicate intentions clearly and invite teamwork and collaboration
- Provide apolitical and non-partisan advice.

Service

- Provide services fairly with a focus on customer needs
- Be flexible, innovative, and reliable in-service delivery
- Engage with the not-for-profit and business sectors to develop and implement service solutions
- Focus on quality while maximising service delivery.

Accountability

- Recruit and promote employees on merit
- Take responsibility for decisions and actions
- Provide transparency to enable public scrutiny
- Observe standards for safety
- Be fiscally responsible and focus on efficient, effective, and prudent use of resources.

These values are at the heart of how we work and, if applied consistently, create a great place to come to work each day. They will also help us to maintain the trust of the public. This Code contains links to a wealth of internal support, assistance and subject experts who can help if you are unsure of your responsibilities. The Public Service Commission website is another source of material on ethics good practice.

Professional standards

We all want to be part of a workplace that helps make NSW a place where people want to live and work, and businesses choose to invest and grow.

To do this we need to perform our roles to the best of our abilities and meet or exceed our commitments by:

- complying with our conditions of employment (which includes having a valid Working with Children Check where necessary)
- including clear deliverables and measures in our performance and development plans
- discussing performance and seeking feedback
- identifying and agreeing with your people leader on what learning and development we need
- using the department's capability development framework and requirements to identify development opportunities and needs.

We need to foster effective collaboration within and between teams. This means:

- contributing to decision-making through open, honest, and timely advice
- once a decision has been made, implementing that decision to the best of our abilities
- complying with reasonable requests from your people leader.

We should take care of ourselves and our workmates. If we are adversely affected by fatigue, alcohol, or other substances, we are unable to perform to the best of our ability and can place ourselves and others at risk.

We must behave in a way that does not damage the reputation of the department or the NSW Public Service. This includes being well presented and courteous when interacting with the public and other organisations.

We should effectively communicate the work the department is doing and how it aligns with the government's position. For this reason, it is important that:

- only authorised employees comment publicly on the activities of the department, including having conversations with journalists or posting on social media
- public speaking engagements are approved before commitments are given

Making the right choices is often complex

If you're in doubt about what to do, ask yourself:

- Do I really feel comfortable with this decision?
- Is it legal?
- Would my family, friends and colleagues be proud of me?
- What impact would my decision have on the department's reputation?
- Would I feel confident explaining my actions to external authorities?
- Would I be happy to be treated this way?

Additional resources are available on the intranet at 'Speaking up and reporting matters'. The Public Service Commission website also has excellent material on [behaving ethically](#).

Work health and safety

Ensuring our people have a safe place to work is a top priority — as is public safety. The department is committed to eliminating and minimising work health and safety (WHS) risks as far as reasonably practicable.

A safe workplace can only be achieved with your help, so we must all:

- be aware of, and implement, the safety systems and practices that help keep each other safe and well
- look for workplace hazards and take action if you see a safety risk — but make sure you keep yourself safe
- report all work health and safety (WHS) incidents, including near misses, within 24 hours on the relevant WHS incident reporting system.

People leaders are expected to:

- lead by example and ensure they model safe work practices
- lead all team members to actively identify safety hazards, assess risk and have in place controls that reduce safety risks faced by our people and the public
- take action if the practices in your team are not consistent with safe work practices
- address any violence in the workplace
- investigate all WHS reports in accordance with department safety systems and implement any new safety measures as soon as practicable.

Find out more about our work health and safety system on the intranet.

Respect and inclusion

Respect and inclusion are fundamental to a harmonious, productive, and psychologically safe workplace where people feel safe to speak up about concerns. We're committed to ensuring our workplace is a safe environment in which everyone feels they can achieve their potential.

The department has no tolerance for harassment or victimisation.

We are all responsible for:

- treating people with dignity and respect, and contributing to a positive and productive workplace
- making sure people feel valued and can fully participate in the workplace
- not discriminating against, harassing, or victimising anyone on any grounds, including:
 - sex, gender identity or sexual orientation
 - marital status
 - pregnancy
 - age
 - race or ethnicity
 - physical or intellectual disability
 - political or religious conviction
- demonstrating inclusive behaviours and using inclusive language
- creating a workplace that is safe and offers protection from sexual, physical, and psychological harassment and neglect

- preventing bullying.

Bullying is behaviour that is repeated, unwelcome and unsolicited. It is considered offensive, intimidating, humiliating, or threatening by the recipient or others who witness the actions or are affected by them.

Bullying does not include reasonable management practices such as performance management and disciplinary procedures, or other reasonable management directions.

The department has no tolerance for bullying.

Examples of bullying behaviour in the workplace

Examples of behaviour that could be considered bullying:

- subjecting another person to ridicule and putting them down in front of colleagues
- using loud and abusive, threatening, or derogatory language
- leaving offensive messages on email or by telephone, SMS, other messaging services and material posted online
- subjecting others to practical jokes that are humiliating, dangerous or offensive.

In a large and diverse workplace there may be differences of opinions or personal standards of acceptable behaviour between colleagues. The department has workplace standards that we all must follow. It is important that we try to resolve these issues calmly, constructively, and promptly.

It's not always easy to do, but there are practical steps you can take to resolve issues. If you haven't been able to resolve an issue, contact your People Partner or lodge a workplace issue.

People leaders set the tone for their teams, and it is important they model good behaviour.

Our people leaders are responsible for:

- demonstrating and regularly discussing the standards of behaviour to make sure the standards are clear and well understood
- supporting employees who speak up and, where necessary, seeking help from your Human Resources People Partner
- understanding the facts and making sure all parties are treated fairly. In complex and sensitive cases an independent investigation may be helpful, and assistance is available
- counselling employees if inappropriate behaviour has occurred, and working to appropriately resolve issues in a way that protects the wellbeing of employees and improves the effectiveness of the team
- providing clear guidance about the standard of behaviour that is expected. If inappropriate behaviour continues, more serious action may be required, and it is important that good records are kept of any relevant conversations
- contacting your Human Resources People Partner if inappropriate behaviour:
 - cannot be resolved to the satisfaction of all parties
 - the potential misconduct is significant; or
 - if the behaviour has happened more than once
- getting further guidance on resolving workplace issues.

Managing conflict of interests

A conflict of interests occurs when an individual's private interests make it difficult to perform official duties impartially in the public interest. Conflicts are common and can arise, for example, from close personal relationships at work, family relationships, social friendships or animosities, and work done outside the department, including volunteering or any political activities.

When we have access to information or are in a position to make decisions, give approvals or authorise expenditure that may benefit or detrimentally affect someone that we have a relationship with, there are possible conflicts of interests. This can include for example, decisions involving recruitment, procurement, community grants or regulatory decisions.

These may be described as:

- **actual conflict** – there is a direct conflict between your current duties and responsibilities and your private interests
- **reasonably perceived conflict** – a person could reasonably perceive that your private interests are likely to improperly influence the performance of your official duties, whether or not this is the case
- **potential conflict** – you have a private interest that could conflict with your official duties in the future.

If we fail to properly manage conflicts, we leave ourselves open to claims of corruption or maladministration. This can affect the reputation of the department and individuals. Conflicts must be declared so they can be managed in a careful and transparent way.

There are a range of ways to handle conflicts, from removing yourself from the affected process to simply ensuring transparency by declaring the relationship. When you consider what action to take, think about things such as the closeness of the relationship and the significance of the benefit or detriment. Find out more about conflicts and ways of managing them on the intranet.

If you believe that you may have a conflict, you must:

- discuss it with either your people leader or the people leader of the affected activity (such as the convener of a recruitment panel or chair of a tender evaluation panel)
- declare the conflict and detail the proposed action to manage it
- comply with the approved course of action for managing the conflict
- always place the public interest over your personal interest.

If you realise you have a conflict of interests that should have been declared previously, you must notify your people leader promptly. It is much easier to fix problems and minimise effects if they are identified early.

If in doubt, protect yourself, your team, and the department by declaring the situation.

People leaders are responsible for promptly considering conflict declarations from their teams and ensuring appropriate management arrangements are in place and documented.

In addition to the above requirements, Resource Regulator staff must also comply with the Regulator's pecuniary interests in the regulated sector policy.

Conflict of duty

A conflict of duty can arise when you can make decisions in more than one functional area. This is sometimes referred to as 'wearing two hats' and can arise for example when a person is responsible for both the area that re-classifies something and the area that regulates change.

If a conflict of duty arises it must be properly documented, and all decisions must be made in an appropriate and transparent way. See conflict of duty page on the intranet.

Senior executive private interests

In addition to declaring any conflicts, all senior executives must make declarations about private financial, business, personal and other interests or relationships that have the potential to influence, or could be perceived to influence, decisions they make or advice they give. If you are acting in a senior executive role for six months or more, you must also make this declaration.

These declarations are made annually and as soon as practicable following:

- any relevant change to your private interests
- commencement in a new role; or
- additional new responsibilities.

See more information about senior executive private interests on the intranet.

Employment outside the department

Experience in other sectors can improve people's contribution to the department. Also, more people are changing from full-time work to more complex and flexible arrangements that better meet their individual needs.

While the department will support staff who wish to perform paid work elsewhere, you must gain approval before accepting paid work. This ensures that there are no conflicts of interests that cannot be managed, and that the extra work will not inappropriately affect your work with the department.

People leaders will determine applications for secondary employment in a timely way and will not unreasonably withhold approval. More information on how to apply is available on the intranet.

Gifts, benefits, and hospitality

Receiving gifts, benefits, or hospitality in the course of your work can be perceived as inappropriately influencing your decisions or actions (such as choosing from which supplier to buy), a conflict of interests or even corruption. This can harm your personal credibility and reputation as well as that of the department. You are required to report offers of gifts, benefits, or hospitality – refer to the intranet.

Offers (other than light refreshment) should be politely refused unless doing so would cause offence, as in the case of meeting with visiting delegations from overseas. If you need to accept an offer, ensure you notify your people leader and complete a declaration form within 10 working days. Your people leader will discuss with you the appropriate course of action.

High-risk areas and activities where you should never accept gifts or benefits include:

- regulatory functions, for example licensing or compliance officers

- procurement and/or disposal of assets
- negotiating and/or managing contracts for public–private partnerships
- administration or approval of grants and similar funding applications
- recruitment
- negotiating and/or managing the delivery of products and services.

See more information on the intranet on what to do if offered a gift, benefit, or hospitality

Flexible workforce

The department promotes a flexible culture that embraces different ways of working. Everyone has the right to request flexible working arrangements that:

- support the needs of the individual, the team, and the department
- maintain or improve services delivery
- uphold our work health and safety standards
- are in harmony with our employment conditions and legislation.

People leaders should consider requests promptly and provide feedback where the proposed arrangement is not considered appropriate.

Leaving the department

Before leaving the department, you must complete several tasks including submitting certain information. This includes when you transfer to another agency or have a temporary secondment. This will help finalise any payments as close to your departure date as possible.

People leaders are responsible for completing the required actions.

We all have an ongoing duty to protect confidential information that we have had access to through our work, which could include departmental information, information generated by another government agency or through a recruitment or procurement process.

Departmental resources

It is vital that we use public money carefully to maintain trust and to maximise cost efficiency.

Every person is responsible for using resources efficiently. While individual decisions about the way we use our resources may have relatively small effects, they all add up. Before using departmental resources ask yourself the following questions:

- Do I really need this?
- Is there a smarter, more efficient way of doing this?
- What is the real long-term cost of doing this – not just the upfront cost? For example, are there maintenance costs, ongoing licensing fees, or extra administration resources needed?
- Am I getting value for money?
- Have I got the right people with the right skills doing the job?
- Am I managing my contracts properly to ensure we get the best outcome?
- Is this consistent with the departments and government's priorities?

If you need more information, please contact your finance team or procurement.

Appropriate use of resources

Departmental resources should only be used for departmental purposes. These resources include things such as vehicles, digital devices, photocopiers, and purchase cards. If you are unsure whether an activity or expenditure is appropriate, have a conversation with your people leader.

For example:

- Providing modest in-kind support for appropriate local community events and charities may be acceptable, with written approval from a senior executive.
- Brief use of the department's phones for personal calls or appropriate use of the internet during breaks is acceptable as long as it does not interfere with work, including that of the people around you.
- Some hospitality and entertainment may be acceptable if it generates direct benefits that contribute to the department achieving its strategic objectives and is approved in writing.
- Paying for employee social events from the department's funds is not appropriate under any circumstance.

To ensure that we have a safe and inclusive workplace, it is important the department's digital devices and tools, including the internet, are not used to create, browse, or download illegal, inappropriate or offensive material.

Departmental resources such as electronic devices and paper files or documents may hold sensitive information or state records and may still have a financial value. Such property should only be disposed of in accordance with the approved procedures.

Budget

Budgets are allocated to ensure that we apply resources in a way that will deliver the department's priorities. It is important that:

- you plan to deliver your functions and participate in the budget process
- once the budget is set, you comply with your budget and budget controls, including net cost of service, gross expense limit, labour expense cap and any capital authorisation expenditure limit.

Sometimes, despite the best planning, circumstances change. If it becomes likely that you will not be able to spend your budget within the agreed timeframe, let your people leader know as soon as possible so the excess funds may be reallocated to priority tasks. Similarly, let your people leader know if you think you may go over your budget. They will provide advice to ensure you can meet your budget target or, where available and appropriate, secure additional funding:

- by a reallocation from within your division or
- from the Chief Financial Officer.

Please contact the finance team for your area for more information.

Buying goods and services

The department routinely buys (procures) goods and services, to help us conduct our business. This can range from routine office supplies to consultancies and contingent labour. It is important for both successful program delivery and our reputation that public money is spent wisely, ensuring we get value-for-money and receive quality goods and/or services. There are a few simple rules that will help you do the right thing:

- **Plan ahead.** For high value, complex, goods or services it is important to plan ahead as the procurement process can take time. Failing to plan ahead can lead to pressure to cut corners down the track. This can include, for example, splitting bills to avoid more rigorous assessment processes or signing a contract before all the details are finalised. Cutting corners is likely to cause problems in the future. It may also be illegal or corrupt and could cost you your employment.
- **Buy the right thing.** This seems obvious, but for more complex purchases it is important to be clear about things such as what is required, when it's required, who is doing the work, the standard of work, and when payments are to be made. Legal Branch can help with the contract, but it is your responsibility to make sure you are buying what you need, when you need it, and to have thought about the risks.
- **Use the right process.** Different procurement requirements apply to ensure probity, transparency, and accountability. The requirements depend on a range of factors such as the type of goods or service, their value, and risk profile. You must comply with these requirements. For some high-value procurements there are also public notice requirements.
- **Understand your budget responsibilities.** You must not agree to buy something unless you have the delegation to spend that amount and you have available budget. To prevent unexpected budget pressures in future years, consider any additional costs that will result from the expenditure, including additional direct recurrent costs, indirect operating costs, and life cycle and future replacement costs.
- **Get help if you need it.** Procurement can be a complex process, but there are subject matter experts who can help. The first contact for procurement questions is your relevant procurement team. Talk to them early. Legal and Finance may also be needed for complex or high-risk matters.
- **Make sure you get what you paid for at the agreed price.** Your responsibilities do not end when you sign the contract. It is critical that before making any payments you check you have received what you have paid for, and at the agreed price. Once you have made

payment it is much harder to rectify any problems. If there is a contract dispute that cannot be appropriately resolved, contact Legal.

Intellectual property and copyright

Whole of government principles apply to the creation, management and use of intellectual property which includes copyright, trademarks, patents, plant breeders' rights and designs

The department owns all intellectual property you create in the course of your work. Anyone who becomes aware of, or suspects misuse of the departments intellectual property must immediately notify their people leader

The department's intellectual property may only be licensed or used by a third party with the relevant approval. Licences for third parties to use Crown copyright will often be free. However, if you think it should be commercially licensed, discuss this with your senior executive or talk to Legal.

If a collaboration with a third party will result in the creation of intellectual property, ownership of the intellectual property should be dealt with in the contract—talk to Legal.

It is also important that we respect and comply with others' intellectual property rights (even if intellectual property material is publicly available on the internet, for example). This includes the cultural material of Aboriginal and Torres Strait Islanders.

You should make yourself familiar with the principles contained in the [Intellectual Property Management Framework for the NSW Government Sector](#) for more information about intellectual property.

Managing grant and funding agreements

If you are responsible for programs that provide grants or other funding you must ensure that:

- program guidelines are approved at an appropriate level, consistent with the decision that established the program
- the guidelines include a probity framework
- the team understands the probity requirements
- funding is being allocated appropriately and consistently with any guidelines and the probity framework
- agreements include terms and conditions that reflect the purpose of the grant or other funding; the department's requirements for reporting, acquittal, and sanctions — if there are any — for breach of the agreement
- grants and funding agreements require ongoing management to ensure that the funds are being applied for the purpose for which they were given.

Managing information

The government promotes the use of information to improve its services and benefit the people of NSW. We are responsible for managing information held by the department, which includes protecting it and making it publicly available under certain circumstances.

Records management

Our decisions can have huge consequences on the whole State, and we need to be able to show how they were arrived at. We do this by creating, capturing and managing records in accordance with the department's records management procedures.

Records may be held in information systems, or they may be in paper or other physical form. Either way, we all need to contribute to protecting records and information held in any information system, digital devices including mobile phones, workplace or storage area used by the department. For example, you should lock your computer if you are leaving it unattended, maintain your own password security and never use other people's passwords.

Digital records must be held in an appropriate business system or in an electronic document and records management system (EDRMS). Physical records are to be stored in a way that protects their integrity and their location recorded in a relevant EDRMS. This is important to enable records to be retrieved when required.

The more significant the decision, meeting or action, the more detailed records should be, including emails, draft and final versions of documents developed on collaborative platforms or elsewhere, meeting minutes and notes of instructions given verbally or via text message.

If you are handling classified information, contact Information and Technology Services for advice on how to follow the correct records procedures. This type of information must not be created, stored, processed, or transmitted within or from the department's information communications and technology (ICT) systems.

The same restrictions do not apply to sensitive information, but you are required to apply the relevant [NSW Government rules for labelling and handling](#).

You must not destroy records unless you're specifically authorised to do so. People leaders are responsible for ensuring:

- employees understand their records management responsibilities, the scope of information and records in their operations and how these should be captured and stored in an approved records system
- employees have access to the records they require to perform their role
- 'vital records' related to their area of responsibility are identified and logged. Vital records are documents that are essential for the ongoing effective functioning of the department. They may include significant long-term agreements, delegations and undertakings to courts or oversight bodies such as the Independent Commission Against Corruption (ICAC) or the NSW Ombudsman.

Confidentiality and privacy

We collect a wide range of business and personal information while carrying out our functions. The public expects us to handle their information carefully, in much the same way as you expect your medical information to be kept private. This means we must have effective safeguards in place to prevent unauthorised or inappropriate use, access, and disclosure of that information.

Breaching confidentiality can seriously harm public trust in us and make it harder to obtain information we need to do our jobs. For business information, breaches of confidentiality may

result in claims for damages. Disclosing personal or health information may be an offence under the Privacy and Personal Information Protection Act 1998 (PIIP Act) and the Health Records and Information Privacy Act 2002.

You should not disclose business or personal information that is not already publicly available, unless this has been approved for release. However, where it is reasonably necessary to advise a complainant of the progress or outcome of a complaint, the PPIP Act (s24) allows for the limited disclosure of some personal information.

More information on confidentiality and privacy is available, but these are the basic principles:

Only release information if you are authorised to do so or have approval.

- Only use information you have access to for departmental work purposes.
- Ensure confidential and personal information is handled in a way that prevents unauthorised access or release. Among other things, you should:
 - build in privacy considerations during the design phase of initiatives. For example, state at the outset whether the department will publish submissions it invites on a public consultation paper
 - consider that confidential information includes Cabinet submissions and associated documentation, and these are provided to employees on a need-to-know basis. More information is available from the department's Cabinet Liaison Officer
- Only collect personal information if it's necessary for a lawful purpose directly related to the department's functions.
- Report breaches of confidentiality or privacy to the Governance Team immediately.

Requests for information

The department receives requests to release information in a number of ways. All formal legal notices should be referred to the Manager Governance & Information as soon as possible via the GIPA mailbox. This includes applications under the Government Information (Public Access) Act 2009 (GIPA Act) and Parliamentary Standing Order 52 notices.

If you are asked to help with an information request, it is important you make rigorous searches for all records relevant to the request. Do this in the required timeframes, ensure all documents within scope are assessed, and provide a thorough response. This provides a complete record in case a response is subject to external scrutiny and comment, for example by Parliament, the NSW Civil and Administrative Tribunal or the Information and Privacy Commission.

People leaders are responsible for:

- certifying that appropriate searches are undertaken and documented
- providing the Information Access and Privacy Unit with information about the documents that may be relevant, whether or not they are released
- advising the minister's office of the potential release of the documents
- providing documents to the Governance & Information team in the required timeframes.

The department often receives informal requests for information about issues that affect or interest people. The department supports transparency, but it is important to ensure that sensitive information (such as personal information, Cabinet documents or commercial information) is not inappropriately released. Advice to help you manage information requests is available.

When we create or receive documents and records, we need to consider whether they will be released to the public. In particular, this includes policy and procedures that describe the way the department makes decisions and delivers services. Wherever possible, documents originating from within the department should be written in the expectation they may be released in some format at some stage.

Cyber security

Cyber security is a rapidly evolving challenge. It is important that we take some simple steps to help protect our systems and information. These include that you:

- don't share or reuse your passwords
- physically secure your device if you are travelling for work with them. This reduces the chance of it being lost or stolen along with all your data
- don't use public Wi-Fi with sensitive data. Cyber criminals can impersonate a legitimate Wi-Fi hotspot, or attack a connection that is not appropriately secured
- think twice before opening email attachments and or links. Phishing emails are becoming increasingly difficult to detect, so be careful when opening email attachments and clicking on the links as it can result in a malware infection, fraud, lost credentials and lost sensitive data
- talk to Cyber-security team before purchasing or using any new information, communications, and technology services, software, or devices to ensure they are secure and meet our cyber security requirements, now and in the future
- report cyber security incidents or breaches to the Cyber-security team

People leaders are responsible for:

- determining what information communication and technology access an employee, contractor or third party (for example a vendor or outsourced business partner) should have. This should be done in consultation with the system owner or relevant ICT Service Centre support
- ensuring employees have the right level of access — no more and no less
- ensuring timely amendment to existing access when employees leave or change their role, including revocation of access where appropriate.

Cyber security incidents should be promptly reported via the intranet.

Making good decisions

We perform important functions that can significantly affect members of the community. For example, we can:

- confer benefits that are not available to everyone (for example, funding grants), and we can also withhold those benefits
- grant access to limited public resources such as fisheries, water resources and Crown land
- exercise enforcement powers that affect people's personal and property rights.

This places us in a position of great trust and carries with it significant responsibilities to carry out those functions in line with the public sector values, legislation, departmental policies and our delegations.

Complying with legislation and policy

Complying with the law and government policy is the right thing to do. The department wants to make it easy for every person to do the right thing and embrace a culture where there is no tolerance for wilful or reckless breaches of the law, policies, or procedures. However, the department also recognises that we operate in a complex legal, policy and process environment where it is not possible for any individual to be an expert in all government requirements.

Subject matter experts have a critical role to play in making information available to ensure we can all do our jobs in a legally compliant way. Subject matter experts will help you to stay up to date as they are responsible for making sure that any changes to requirements are reflected in our policies, our procedures and any information developed for employees and the community. Subject matter experts should ensure that guidance material:

- has been approved at an appropriate level
- is concise, customer-focussed, in plain English and accurate
- has been prepared in consultation and collaboration with related content owners and updated to reflect feedback from users
- has been communicated to those in the department most affected by the change
- remains accessible and updated as required.

Subject matter experts exist both in operational and corporate areas. **Anyone** may be a subject matter expert. It is important every person understands who subject experts are, how they can help and, if you are one, your responsibilities.

Refer to Attachment A for the list of subject matter experts related to this Code.

Who is responsible for compliance?

It is everyone's responsibility to do the right thing and comply with our legal and policy responsibilities. If you are not sure about an issue, ask your people leader or a subject matter expert.

People leaders have an important role to play in ensuring their teams are made aware of legal, policy and budget responsibilities including their delegated powers.

What happens in the event of a breach?

Breaches can indicate where further guidance or training may be beneficial or that policies or procedures need clarification. Subject matter experts are responsible for tracking breaches in their area of responsibility and escalating significant or systemic problems so that action can be taken.

You should report to your people leader if there has been a breach. It is often easier to resolve issues earlier rather than later.

Risk management

The department aims to create a positive and risk-aware culture within a robust risk management framework that supports the clear and transparent understanding and management of risks.

Risk management is the process of anticipating future events that could adversely affect the department and acting to either reduce the likelihood of the risk occurring or reduce the consequences if the risk does occur.

The key reasons why we need to manage our risks are to:

- improve the likelihood of achieving our strategic and business objectives
- proactively identify and manage opportunities and threats
- improve stakeholder confidence and trust
- improve loss prevention and incident management
- enhance organisational learning and resilience
- provide an effective basis for decision-making and planning.

Everyone is responsible for identifying and acting on risks. Frontline employees are the people most likely to see operational risks early and the department needs your help to capture these.

You have a responsibility to embrace the management of risk, which includes:

- adhering to departmental policies and procedures
- undertaking appropriate risk education
- embedding and applying key risk-management processes and practices within your group.

People leaders are responsible for:

- ensuring their team is encouraged and feels empowered to raise and discuss potential risks
- identifying and recording emerging risks or changes that require existing risks or their controls to be reframed or re-evaluated
- monitoring controls to ensure they are being implemented and are effective
- ensuring their team is aware of the risks and controls in place
- minimum six-monthly reviews, or reviews when a material change in business conditions, operations or environmental context could arise or is experienced.

To ensure risks are handled and reported consistently, the department has developed risk management policy and guidelines, which we are all required to implement.

Business improvement – audits, inquiries, and investigations

We can identify problems with, and opportunities to improve, our systems and processes through a number of mechanisms. Reviews such as audits, inquiries or investigations often result in improvement recommendations. While the department does not need to accept all recommendations, it must give due consideration to insights and recommendations and respond appropriately. If we know about the problems and do not act on them, we face significant reputational damage if a problem arises later.

People leaders are expected to:

- provide informed and prompt responses to auditors and investigators

- record the anticipated delivery date of the review
- ensure there is a formal response to the recommendations within 30 days or as approved by the Secretary
- ensure required actions are logged and monitored through to completion.

Senior executives need to make decisions about the required action and ensure any action needed is carried out in a timely manner.

Engaging with the community

We as public servants manage a range of programs, and it is our responsibility to engage and seek the views of the community. This occurs through the following:

- formal consultation processes
- meeting with interested parties
- directly with our customers
- sponsorship programs to inform the community

We need to be clear about how we engage with the community to ensure standards are upheld and public expectations are met.

Stakeholder engagement

Stakeholder engagement ensures the people of NSW have the opportunity to contribute to government decisions. It helps us develop and implement good policy. Approved engagement activities provide an opportunity to deliver better public policy and can also help us identify opportunities to improve service delivery and customer satisfaction.

When we engage with our stakeholders, it is important to acknowledge that their needs vary, and we must use a range of engagement approaches to ensure all views are understood and represented.

Engagement activities should be tailored to help get the best input from the stakeholders, and arrangements should be documented and have appropriate approval.

Lobbyists

The department recognises the need to make important decisions in an open and transparent manner, without any real or perceived undue influence from external parties.

There are obligations on parties seeking to influence decisions and outcomes, and on the departmental officers they interact with, to ensure any interactions are transparent, properly recorded and don't involve or have the perception of exerting undue influence.

The rules about third-party lobbyists are available on the intranet.

Managing complaints about the services we provide

As taxpayers we expect government to provide good services. As public servants we aim to provide high-quality, seamless services to our external stakeholders and customers. This includes those who access or are affected by the programs and services we deliver.

We offer our stakeholders and customers the option to provide us with a compliment, suggestion, or complaint. We welcome all feedback. Understanding the cause of complaints gives us an opportunity to improve our services and often address issues we didn't even know were occurring.

From time to time, we receive complaints that are an expression of dissatisfaction made about us, our services, or our employees where a response or resolution is explicitly or implicitly expected. In handling complaints, we have adopted the NSW Government's [six complaint handling commitments](#).

Complaints can be received through various methods, including but not limited to; email, online form (Feedback Assist), in person, in writing or by phone. It is better to resolve a service complaint at the frontline, preferably through discussion. If this is not possible and the complaint is received through means other than Feedback Assist, the details need to be entered in to Feedback Assist

by the receiving staff member, who will then email an acknowledgment and case number to the complainant and directs the complaint to the relevant business area for assessment, referral, and resolution. Each complaint issue will be addressed, and improvement opportunities identified and addressed.

This is easily done through the 'Your Feedback' widget on the right-hand side of the department's main webpage and the webpages of all other NSW Government agencies. This allows us to respond to concerns raised in a consistent, timely and cost-effective way.

Sponsorships

A sponsorship is a commercial arrangement in which a sponsor provides money or in-kind support in return for benefits such as improved relationships, enhanced profile, or association with a program or initiative. A sponsor generally expects to receive a benefit beyond a modest acknowledgement.

We do not use sponsorship as a primary tool to conduct our business, irrespective of whether we would be receiving or granting the sponsorship. It may be appropriate if the activity directly contributes to government priorities if it directly aligns with the department's documented strategic objectives and does not create an inappropriate conflict.

Sponsorship proposals are evaluated in line with ICAC's [sponsorship principles](#). Further information is available on our sponsorship page.

Speaking up and reporting matters

We can only resolve problems and put improvements in place if people speak up.

Our leaders will support people who speak up by listening and providing feedback on the actions they have taken and the reasons for these actions. Speaking up is more likely to be effective if it takes place early and in a constructive, courteous way.

Practical tips

There are a number of reasons why people don't speak up. Simple tips for overcoming those reasons are listed below.

- 'I raised it before and no-one did anything, so what's the point?' Make sure you listen to your team, let them know what you are going to do and then do it.
- 'That's just the way it's always been done around here.' This is never a good enough reason for anything.
- 'I'm junior so why would anyone listen to me?' Good ideas can come from all levels and a good leader listens to everyone in their team.
- 'I'm new so why would anyone listen to me?' When you are new you can see with fresh eyes problems that people have grown used to.
- 'I'm scared I might be judged and that it might limit my career.' There are no stupid questions. If you don't understand a decision, it's your leader's responsibility to explain it.

Confidential reporting options and requirements

Sometimes speaking up can be difficult, and discussions at the local level are not always effective or appropriate. If you are concerned about raising a matter at a local level, or previous attempts to resolve it at that level have not been effective, you can:

- talk to your people partner or the Governance & Investigations team about strategies for more effectively raising issues
- anonymously report via the online reporting form, which allows employees or members of the public to lodge reports about suspected fraud and other serious misconduct
- lodge a public interest disclosure to get protection under the [Public Interest Disclosure Act 1994](#)
- contact the [NSW Ombudsman](#), [Independent Commission Against Corruption \(ICAC\)](#), [Audit Office of NSW](#) or the [Information and Privacy Commission](#)
- get practical guide for resolving other workplace issues.

If you require ethical advice you can contact Ethicall via the intranet, a free, confidential external ethics helpline.

All employees must:

- report WHS incidents within 24 hours
- report any suspected corrupt conduct, maladministration, or fraud to the Director Governance, Information and Privacy or through one of the options listed above.

People leaders are responsible for:

- supporting their team members in raising concerns and providing constructive guidance
- acting if they see behaviours in their team that do not support people speaking up
- ensuring that they and their team are aware of their responsibilities under the [Public Interest Disclosures Act 1994](#)
- reporting all breaches or potential breaches of the law to the General Counsel
- reporting all breaches of policy to the relevant subject matter expert
- reporting unresolved or repeat misconduct, including bullying, harassment, or discrimination, to the People team
- recording new or changing risks and unresolved issues.

Fraud, corruption, and maladministration

The department has no tolerance for fraud, corrupt behaviour, or maladministration. You must report all reasonably suspected instances of wrongdoing.

Wrongdoing includes:

- corrupt behaviour
- maladministration
- serious and substantial waste of money
- breach of the GIPA Act
- local government pecuniary interest contravention (by council officials only).

Different parts of the department may have specific fraud and corruption controls, depending on the nature of the functions and the level of risk. Make sure you're aware of and comply with any fraud and corruption controls that apply to your work area.

If you are contacted by the ICAC or NSW Ombudsman, you should refer this to the General Counsel or the Director of Governance, Information & Privacy.

Senior executives are responsible for ensuring that fraud and corruption risks are regularly reviewed in their area of responsibility. In medium- and high-risk areas, such as procurement, funding and grant delivery, payroll, systems administration and regulatory functions, senior executives must document the controls in place to manage fraud and corruption risk and ensure these controls are kept up to date.

Fraud can include simple things such as paying for personal items with your purchase card; falsifying your timesheets about how many hours you have worked and using work resources for personal purposes.

Examples of **corruption** include theft, bribery, selling confidential departmental information, manipulating recruitment decisions, or accepting a gift in exchange for issuing a permit.

Maladministration includes acting without authority – for example, approving a purchase beyond your approved dollar limit. Another example is where rules or procedures that are intended to guide decision-making on granting licences have not been applied correctly.

You can find more fraud, corruption and maladministration information and guidance on the intranet.

Criminal offences and bankruptcy

If you are charged with, or convicted of, an offence punishable by imprisonment for 12 months or more, you are required to notify the Secretary, even if the offence was committed in your private capacity. You are also required to notify the Secretary or delegate if you are declared bankrupt or enter into an arrangement with creditors. If a less serious criminal charge is brought against you, you should raise this with your people leader if it may affect how you do your job.

Breach of the Code

The Code sets out the ethical and behavioural standards you are expected to demonstrate while working for the department. If you fail to meet those standards, corrective action may be taken in accordance with the *Government Sector Employment Act 2013*.

If there is a finding of misconduct, the action taken will depend on the circumstances, but may include caution or reprimand, assignment to another role, a fine, reduction in grade or termination of employment.

Computer and other workplace surveillance

The department undertakes continuous and ongoing surveillance of workplace systems and equipment in accordance with the *Workplace Surveillance Act 2005*. This may include reviewing departmental closed-circuit television, email accounts, electronic files and internet usage on work computers and mobile devices such as tablets and smartphones. As the department's vehicle telematics system has a location and usage reporting capability, it is also a form of workplace surveillance.

The department can use the information to:

- monitor compliance with the Code and other departmental requirements
- identify conduct that may be illegal or adversely affect the department or employees
- investigate non-compliance matters such as illegal, inappropriate, or excessive personal use
- support safe workplaces, identify at-risk behaviour, and simplify reporting requirements
- protect the department's information, people, assets, property, and finances.

It is important to note the information is only used when requested under appropriate authority.

How to contact our subject matter experts

Use our contact list to find a subject matter expert for topics or functions in relation to the Code of Ethics and Conduct.

Function	Subject matter expert
Bullying, discrimination, & harassment	Director HR Business Partners and Industrial Relations
Code of Ethics and Conduct	Director Governance, Information and Privacy
Conflict of interest + other declarations under the Code	Director Governance, Information and Privacy
Cyber security	Chief ICT Officer
Finance	Director Finance Operations
Fraud & Corruption	Director Audit and Risk
Fraud – investigations	Director Governance, Information Privacy
ICAC/NSW Ombudsman	Director Governance, Information and Privacy
Information requests- GIPA, SO52, & Subpoena	Director Governance, Information and Privacy
<i>Operational policy & procedures</i>	<i>Relevant operational area</i>
Privacy, including privacy complaints	Director Governance, Information and Privacy
Procurement	Chief Procurement Officer
Public comments, social media, & publishing	Director Media & Communications
Public interest disclosures	Director Governance, Information and Privacy
Purchase Cards	Director Finance Operations
Records management	Chief ICT Officer
Risk management	Director Audit and Risk
Secondary or private employment	Director Governance, Information and Privacy
Work, health, & safety	Director Health and Safety