



HM Government



- Setting standards and policy
- Building a profession
- Better use of data
- Reducing harm and loss

# Government Counter Fraud Profession Code of Ethics & Conduct

January 2017

## Introduction

The general standards of personal and business conduct that everyone in public service is expected to uphold are set out in their Employee Code of Conduct, issued by Human Resources. For those in the Civil Service, this is the **Civil Service Code**.

This Code sets out enhanced standards of professional behaviour that are specific to the Government Counter Fraud Profession, in consequence of the unique role its members play in reducing fraudulent activity against the public sector.

The counter fraud profession in government has a key role in championing good governance, to safeguard public funds and maintain public confidence. Those working in the profession must actively promote and demonstrate sound ethical behaviour in all parts of their life, to ensure the profession is not brought into disrepute.

## Core Principles

We, like all public servants must perform our roles whilst maintaining a high degree of integrity and reliability to ensure public confidence.

All counter fraud staff are expected to uphold the following values by consistently demonstrating high standards of professional behaviour, both in their organisations and when representing the profession to outside organisations and the general public.

The core principles observed by those in the profession are aligned to those of the Civil Service:

- Integrity
- Impartiality
- Objectivity
- Honesty

## Observing Our Code

This code supports civil service policies and values. Everyone in the profession has a responsibility to observe the provisions of this code and ensure it is honoured at all times.

Strict observance of this code will ensure a consistent and professional approach to combatting fraud whilst maintaining the confidence of colleagues, stakeholders and the public.

We have a shared responsibility to ensure that the way we conduct ourselves promotes these core principles, which underpin how we work with those we come into contact with.

These principles should underpin every decision made and every action taken in countering fraud and other economic crime.

These principles should also be used to consider behaviour and conduct in day-to-day work, recruitment, procurement, training processes and performance reviews with staff.

## General Responsibilities

The nature of the counter fraud profession means that there is often a requirement to work autonomously. As a consequence we hold a position that requires us to be trustworthy and act accordingly at all times. Should a member of our profession fail to meet the high standards expected, it follows that it is likely to be regarded in a more serious light than if they had occupied a position of lower responsibility.

## Professional Approach

Our profession is responsible for developing an effective response to fraud through the utilisation of professional standards and values, combined with an awareness of possible commercial interests and sensitivities. Managing our approach correctly will reduce the risk of further financial loss and reputational damage.

Any compromise of these standards may have a detrimental effect on Government and/or a third parties credibility and could undoubtedly prove more costly in the long term.

**Inconsiderate and irresponsible actions can have a significant impact on our profession, the Government, the wider public sector and the UK, not only in financial but also reputational terms.**

**These could include:**

- **Not considering disruption to frontline services in your approach/response to counter fraud.**
- **Treating the information you handle insensitively**
- **Failure to consider commercial interests and sensitivities**

## Tact and Discretion

Applying firm measures to combat fraud does not mean that people or organisations are treated in an unacceptable way. We must always endeavour to use tact and discretion in dealing with, and disseminating information about organisations or individuals when, for example, identifying fraud risks. We must ensure that those we come into contact with are treated with courtesy and respect; be clear and determined in our actions; remain professional at all times.

We must at all times maintain the highest standards of personal conduct and integrity; exercise self-discipline, be discreet and always act within the law.

We will sometimes have access to a high level of sensitive information. Absolute discretion is essential, as any compromise of this information may cause serious damage to government, other public authority interests or a member of the public.

### Have you considered?

- **Disclosing sensitive personal data, such as allegations of crime against someone, can result in a £500k fine from the Information Commissioner's Office.**
- **Prosecutions against those charged with fraud could be compromised if the Court finds that the investigators conduct was overbearing or abusive towards a suspect or witness.**
- **Openly discussing in public identified fraud risks, or weaknesses in controls, could lead to an increase in fraud loss as the information could be used to further undermine controls or exploit loopholes.**

**We must ensure that the impact of disclosure of information - either accidentally or deliberately - does not breach the law, such as the Official Secrets Act, compromise security or bring our profession into disrepute.**

## Accountable for Quality

We are accountable for the quality of our work and we must take responsibility for maintaining and improving our knowledge and skills. As a professional member we should drive for quality in everything that we do and in those who support our counter fraud work.

## Fairness and Objectivity

In all dealings we should maintain an open, impartial and objective outlook. This is particularly important whether assessing, handling, and disclosing evidence or running a recruitment campaign or procurement exercise. Processes should be open and fair, with rationales for decisions documented clearly.

In addition, we must always be mindful of the rights of others, ensuring that people are not discriminated against because of their age, disability, gender, race, religion, beliefs or sexual orientation.

## Our Standards

Alongside this Code, the Government Counter Fraud Profession have approved a set of standards for specialists working in counter fraud that outline the skills and competencies required to be proficient in each specialism.

Counter Fraud Awareness standards are also being developed, targeted at different roles in the public sector including all staff, Board level individuals, grant makers and policy staff.

## Unconscious Bias

Certain situations will exacerbate our biases. This may be because we feel tired, stressed, threatened, frustrated or anxious.

### What can you do?

Challenge yourself with these questions:

- Is my belief always true?
- Do I have any evidence of it?
- Where did this idea come from?
- Am I being logical?
- Are there any exceptions?

## Behaviours we expect to see:

- **Courageous:** Standing up for what is right, never ignoring unethical or unprofessional behaviour. Having the courage to hold difficult conversations with stakeholders to ensure the best outcomes.
- **Challenging:** To challenge appropriately where the wrong decision is being made or inappropriate behaviour e.g. bullying, indiscretion etc. is being displayed.
- **Collaborative:** Partnering and collaborating with the wider fraud community and stakeholders within your organisation.
- **Objective:** Acting solely according to the merits of a task and serving governments with different objectives with a commitment to objectivity and impartiality.

## Example Behaviours: *Courage*

The understanding of fraud and its presence in public organisations is not always understood. As a professional, responsible for championing good governance, you should use your knowledge and expertise to inform and educate senior leaders and other professionals. You must be persistent but professional in managing stakeholders.

**Doing it differently** – just because its “*never been done before*” does not mean it cannot be done. Challenge the illogical, engage with those who should know and be vigorous in defending the role of counter fraud. Work with legal advisors to develop new sanctions, and understand how to apply legislation to tackle fraud effectively. Be legislatively audacious and use the law in imaginative ways to tackle fraud.

## Example Behaviours: *Challenging*

Our profession sometimes exposes us to working practices that do not meet our professional values and conduct. We have a duty to raise these conflicts in the most suitable way with those who are responsible.

**Dishonesty is not the best policy** – avoiding the awkward truth does not resolve unethical practice. Always be conscious of your working environment and challenge any poor practice.

## Behaviours Example: *Collaborative*

Fraud evolves regularly and we must too. Working together for a common purpose promotes imaginative ways of reducing fraud and supporting an effective counter-fraud culture. Collaboration is important between different business units (such as HR, Audit and Legal), when considering fraud risks or achieving sanctions, as well as collaboration within the profession.

## Behaviours Example: *Objective*

It is imperative in counter fraud to remain objective at all times. This is equally important whether designing a fraud response plan, developing a strategy, interviewing, considering sanctions or engaging with key stakeholders. We must aim to be aware of how our 'unconscious bias' can influence our decisions and actions and ensure that these do not impact adversely on the facts or tasks in hand.

## Our lives have never been so open.

### Have you considered?

- Your 'online' profiles – do they reflect you and your professional profile accurately?
- Your 'online' activity or mobile communications - what you say to others about your work and what you reveal in social media.
- The security settings of both your personal and work based social media accounts (as applicable) and how you brief your staff on being safe and keeping information secure online.