

# Top tips for preventing, detecting and responding to fraud: a checklist

This checklist is reproduced from Tackling fraud in the charity sector: making your money count, a special report by the Fraud Advisory Panel and Charity Commission. It highlights the main learning points from the first national conference on charity fraud held in late 2015, available from [fraudadvisorypanel.org](http://fraudadvisorypanel.org) and [charitiesagainstfraud.org.uk](http://charitiesagainstfraud.org.uk)

## GOOD GOVERNANCE AND FRAUD RISK MANAGEMENT

---

- Prevention is better than cure – and much more cost-effective! Review your processes and procedures and introduce strict accountability to make it hard for anyone to commit fraud in the first place. Never use trust as an excuse for poor risk management.
- Fighting fraud is a job for everyone at every level. Make the in-house case for an ethics programme by focusing on positive behaviours – doing the right thing, setting the right tone, leading by example, supporting staff, building a good reputation – and emphasising the wider benefits.
- Make sure your trustees treat fraud awareness and risk management seriously. Systematically encourage fraud awareness and understanding throughout your organisation.
- Create a framework of strong values and then publicise them in a formal code of ethics. Include examples of day-to-day ethical business dilemmas to help employees and volunteers understand what is at stake and to make good decisions under pressure.
- Understand the risks you face by conducting an annual fraud risk review and then documenting areas of greatest vulnerability in a risk register. Some fraud is inevitable so be clear about how much fraud you are prepared to tolerate (your charity's 'appetite' for fraud risk) and manage the risks accordingly. Have regular and frank conversations with your delivery partners about fraud risks and reporting.



- Conduct process test checks, especially on vulnerable systems. Watch key procedures, such as the opening of post, and do not make assumptions. Do you know how easy is it to change the destination account on your direct debit run? Are your fundraisers following up sponsorship forms that are not returned? Train your supporter care teams properly so that they will recognise fundraising fraud red flags when they see them.
- Adopt a clear and unambiguous whistleblowing (or 'speak up') policy. Give it plenty of support and publicity. Write it with the typical concerns of employees in mind. Who should they talk to? Will something really be done? Are reports truly confidential? How will you prevent retaliation?

### PEOPLE: YOUR GREATEST ASSET OR WEAKEST LINK?

- Build a workplace culture in which fraud is never acceptable and everyone knows it. Use your anti-fraud policy to explain this to everyone.
- Replace high levels of trust with high levels of accountability and professionalism. Know what people are doing in your name; keep good records and keep an eye out for oddities and anomalies. Tackle fundraising threats with well-managed controls and good record keeping.
- Remember, where there's cash there's temptation. Find ways to make it easy for staff to do the right thing. Develop standard operating procedures that reduce risk and encourage honesty.
- Get to know your staff and volunteers better. Run pre-employment screening of new recruits as well as in-service checks for established employees – and expect your partners to do the same. Share your knowledge with other organisations so that known fraudsters can't job-hop.
- Offer support to employees in difficulty. Desperation and dissatisfaction are common causes of fraud.

### UNDERSTANDING AND PREVENTING COMMON FRAUD RISKS

- Understand your financial systems and data (including payroll and direct debit donations) and get to know what 'normal' looks like so that you can recognise the signs of fraud when you see them.
- When setting up a new office or starting a new project undertake a fraud risk assessment to make sure control systems mitigate actual risks not theoretical or anecdotal ones. Periodic follow-ups will keep things fit for purpose.
- Check that managers really are applying and monitoring your charity's financial and other controls.
- Make sure staff and volunteers who stand up to fraud, bribery and corruption are properly protected.
- If you are truly committed to tackling corruption there will be operational disruptions, so plan for them. Be determined; the eventual rewards will be worth it.
- Educate staff in good online 'hygiene'; be suspicious of websites with mistakes or odd URLs and treat with caution unfamiliar emails containing links and attachments (as well as familiar emails containing unfamiliar links).
- Bring password protocols up to best practice standards. GCHQ now says frequent, compulsory password changes result in less secure passwords.
- Protect staff mobile devices, laptops and PCs with anti-virus and anti-spyware software that is kept up-to-date.
- Encrypt all devices that transfer or receive data containing sensitive and personal material. (There could be implications under ss.7 and 55 of the Data Protection Act 1998.)

