TACKLING CHARITY FRAUD CHECKLIST

This checklist should be read in conjunction with *Tackling fraud in the charity sector: prevention is better than cure*, a special report by the Fraud Advisory Panel and Charity Commission, available from **www.fraudadvisorypanel.org and www.gov.uk**

GOOD GOVERNANCE

WIN BOARD-LEVEL SUPPORT

- [ ] Appoint a counter-fraud champion from your senior management team to influence and drive change widely throughout the organisation.
- [ ] Use case studies and other real-life examples to make sure senior management really understands the fraud threat as well as the reputational damage that faces any organisation ill-equipped to deal with a fraud or cyber-attack.
- [ ] To minimise the risk of nasty surprises and to build widespread trust, create a structured process for reporting on fraud and anti-fraud activities to senior management and board members.

TACKLING CYBERCRIME

CYBER SECURITY

- [ ] Deploy the most up-to-date computer security software available, including network firewalls. Never simply assume that technology will do its job; it is crucial to remain vigilant. The number of criminals with computer expertise continues to grow and many fraudsters now have the ability to bypass online defences.
- [ ] Avoid printing hardcopies of personal information – they make it even easier for criminals to get their hands on other people's personal data.
- [ ] Complete the online self-assessment questionnaire at **www.cyberessentials.ncsc.gov.uk/**. It will help your organisation understand those areas of your cyber security that require further controls and safeguards.

PROTECTING YOUR INFORMATION

- [ ] Make sure you know what information you are holding and why. Look beyond the obvious sources and systems. Remember, if the ICO comes calling, ignorance will be no defence.
- [ ] Proper governance, competent and engaged staff and rigorous processes are all as important as technology when it comes to protecting information.
- [ ] Take great care when specifying your IT systems; understand what the software does, keep good records and make IT contractors subject to robust contracts.
- [ ] Warn staff and volunteers about the dangers of free public WiFi and encourage the use of a VPN and/or encryption to protect sensitive information.

INSURANCE

- [ ] Create a full picture of on- and offline fraud risks.
- [ ] Consider whether risks would be better transferred to an insurer.
- [ ] If appropriate, speak to your broker about options.

COMMON FRAUDS AND HOW TO PREVENT THEM

GRANT FRAUD

- [ ] Encourage grant holders to be open and honest. Make clear what is expected of them.
- [ ] At the application stage take the time to get to know and understand applicant organisations, their people and projects. Verify the identities of key individuals and use public sources, such as the Charity Commission and Companies House, to check other information provided on the application form and supporting documents.
- [ ] Once a grant has been awarded, monitor the project and how the funds are being spent. Watch out for bogus monitoring information and consider regular, comprehensive auditing of a sample of grant recipients.

BANK FRAUD

- [ ] Regularly review and update online payments system-user roles and privileges.
- [ ] Do not share banking passwords and make certain they are changed regularly.
- [ ] Apply payment limits and strictly enforce dual authorisation of payments.
- [ ] Question all requests for information, especially when unsolicited/unexpected. Don't be rushed or pressured into making a hasty transaction.

PROCUREMENT FRAUD

- [ ] Appoint a contract manager (or some other designated person) to take responsibility for all contracts.
- [ ] Verify supplier performance and pay only for what's actually been received – that means monitoring and auditing deliveries of goods and confirming the successful provision of services.
- [ ] Seek independent verification of any requests to vary payee details, using an entirely different communication channel to the original request.
- [ ] Audit all procurement processes. Monitor and review the performance of anyone responsible for contract management.

FRAUD ADVISORY PANEL

CHARITY COMMISSION FOR ENGLAND AND WALES

SUPPORTED BY Crowe Clark Whitehill™

A Member of Crowe Horwath International

DETECTING FRAUD

FRAUD REPORTING SYSTEMS

- [ ] Having a well-communicated anti-fraud policy is an easy and effective way to demonstrate the right tone at the top.
- [ ] Assess whether your reporting mechanisms are easy to access and operate by everyone, everywhere.
- [ ] Create a staff guide to reporting concerns which explains the what, why, where, how and to whom.

STAFF AWARENESS AND TRAINING

- [ ] Listen to your people, gather their feedback, and act on it. Be aware that staff may be reluctant to share experiences that might implicate them or their colleagues, particularly if there could be disciplinary or legal implications.
- [ ] Tap into the expertise of colleagues in other business areas (such as IT, public relations or brand) to help develop new ways to engage with staff.
- [ ] Monitor the success or otherwise of your new programmes by focusing on Key Performance Indicators (KPIs). If you can, use established, familiar mechanisms (such as staff surveys) to gather the information you need.

DATA MINING

- [ ] Document the full extent of your data 'universe' and make sure any data mining is consistent with the GDPR.
- [ ] Check the contractual arrangements governing your back office systems. If they are outsourced make sure you have access to your own data whenever you want it and at no cost.
- [ ] Create a fraud risk register and use it, in conjunction with in-house knowledge, to create a full risk profile which can then be tested against the data. Look for things like collusion (between employees, volunteers and suppliers), bogus grant applications, and donations to partners in high-risk locations.
- [ ] Match key information across employees, volunteers and suppliers – things like addresses, bank sort codes and account numbers, telephone numbers and email addresses – looking for anything suspicious (including conspicuous perfection). Independently validate addresses, company/charity details and social media footprints for anyone mentioned in a grant application, then data match them against the financial regulators' sanctions lists.

RESPONDING TO FRAUD

REPORTING FRAUD

- [ ] Report all actual or attempted fraud/cybercrime to Action Fraud.
- [ ] Report all serious frauds to the Charity Commission, explaining what has happened and what's being done to deal with matters.
- [ ] Speak to the City of London Police if you are planning a major fundraising event. They can create a key-word alert to flag up anything new online that appears related to your charity, and then work with you to take down imposters.

CHARITY COMMISSION INVOLVEMENT

- [ ] Review your internal financial controls and complete the self-assessment checklist to evaluate your charity's performance against legal requirements and good practice recommendations.
- [ ] Know your duties and responsibilities and make sure that everyone has read the ***Essential Trustee.***
- [ ] Consider the top 10 tips to protect your charity from fraud, available in the compliance toolkit ***Protecting Charities from Harm*** (chapter three: fraud and financial crime).

DEALING WITH THE MEDIA

- [ ] Prepare for the worst so that you are always ready to communicate constructively about a fraud event or cyber-attack as soon as it is discovered or reported. Plan and prepare in advance as much of your media response as you can.
- [ ] Follow the three key principles of effective media communications: timeliness, completeness and cooperativeness.
- [ ] Don't comment on the fraud-related problems of other charities.

CIVIL ACTION

- [ ] To recover unpaid donations consider action in the civil courts. It's easy, low cost and effective.
- [ ] To start civil actions online use HM Courts & Tribunal Service's ***Money Claim Online***, which enables the whole process to be easily self-managed.
- [ ] Establish whether the case is suitable for civil action. There should be strong evidence of wrongdoing and the suspect should have received at least two letters about the missing funds to which they have not replied.

TACKLING CHARITY FRAUD
PREVENTION IS BETTER THAN CURE