TACKLING GRANT FRAUD

A GUIDE TO HELP FOUNDATIONS DETER AND DETECT FRAUD

May 2020

This guide offers an update to *Tackling External Grant Fraud*, published by ACF in 2008. Based on the principles of good practice, it incorporates recent changes in regulation, legislation, and support as well as developments in digital technology and ways of operating.

All organisations are at risk of fraud. Research which informed the earlier version of this guide found that foundations were particularly vulnerable to grant fraud due to a combination of being known to distribute funding and being seen as 'benign' charitable organisations. Several members identified that they had been dishonestly approached for relatively small sums of money through normal application processes. In response, some foundations reviewed their existing procedures, identifying fraud risks and implementing mitigating controls. Other organisations felt their controls were sufficient, while others felt that fraud would not happen to them. This is a high-risk position to take; when other organisations take significant steps to prevent fraud, those that don't become easier targets.

A Grant Risk Management Project was set up to raise awareness of the issue of fraud and develop standards of good practice. It was supported by a consortium of members and led by a project officer. This project culminated in the publication of *Tackling Grant Fraud 2008*.

Much of the content in the 2008 publication is still relevant today, but changes in the grant-making landscape and in society have brought new issues and challenges when it comes to preventing fraud. ACF has updated the guidance in 2020 by building on the original publication and adding new sections, drafted in consultation with Phil Sapey Associates.

The focus of this publication is grant fraud, but measures should be taken as part of a wider approach to due diligence, mitigating risk and protecting the foundation's resources. This guide should be read alongside other resources that take into account other types of fraud to which all organisations are vulnerable.

CONTENTS

1. INTRODUCTION

Why fraud matters

Fraud can divert resources from the aims of the organisation, meaning genuine beneficiaries get less support or go without. In addition to loss of finances, fraud can damage the reputation of an organisation, but it is vitally important to remember that trustees have a legal duty to look after foundation funds. The Charity Commission for England and Wales[1] and the Scottish Charity Regulator (OSCR)[2] explain that trustees have a responsibility under charity law to protect the funds and other property of their charity. Trustees must also comply with the general law (and overseas law where applicable) including in relation to the prevention of fraud, money laundering and terrorist financing. Fraud will flourish in an environment of weak governance and poor financial management. This means that the protection of charity funds begins with robust financial control systems within a framework of strong and effective governance. Beyond compliance, preventing against fraud ensures that the foundation's resources, not only financial but also time and capacity, are deployed to best effect in pursuit of the foundation's objectives.

Fraud matters beyond its impact on the individual foundation. Charities have faced increasing public scrutiny in recent years of the way they deploy and manage their resources. Debates about overheads, executive pay, fundraising methods, investment policies and grants decisions have contributed to public and regulatory interest in charity resources being used appropriately and effectively. Taking measures to protect against fraud helps to build public confidence and to maintain the charity's reputation.

Fraud against charities takes many forms including:

- Fraudulent beneficiaries
- Bogus fundraisers
- Cyber-crime
- Fake charities
- Employee fraud
- Fraudulent grant applicants
- Procurement fraud
- Invoice fraud[3]

Criminals do not discriminate, targeting any organisation where they perceive controls are weak and gains significant. This includes cyber-criminals who take advantage of vulnerabilities in systems, but

[1] Charity Commission for England and Wales (2016) *Compliance toolkit: Protecting charities from harm*, Chapter 3: Fraud and Financial Crime – summary: https://bit.ly/CCEW-toolkit-fraud
[2] OSCR (2018) *Charity trustee duties and fraud prevention*: https://bit.ly/OSCR-fraudprevention
[3] Invoice fraud can include the submission of false or duplicate invoices to your organisation from genuine or fake suppliers. They might also form part of grant application or monitoring information.

more often, it is a lack of staff training that means people can be duped into clicking on links that lead to malicious software.

We recognise that most grant applications are honest. There are occasionally innocent mistakes made by trustworthy individuals and organisations. However, it is important not to be naïve to the fact that the actions of a dishonest minority can have a significant effect on the whole charity sector. Research suggests that fraud could be costing the charity sector hundreds of millions, and possibility billions, of pounds each year[4]. Further research has not been published, but it is hard to believe this estimate will have decreased. It is recognised that measuring fraud loss is difficult for a number of reasons, including the fact that fraud is a hidden crime and it may not have been identified, and that organisations have different definitions of fraud and record losses to fraud differently. Any incident of fraud can be hugely damaging and costly to the charity and beneficiaries, and so it is essential to take steps to prevent it.

What is grant fraud?

For the purpose of this guide, we consider grant fraud as the dishonest application or deliberate misuse of grant funding by an individual or organisation external to the foundation.

Grant fraud is just one type of fraud. Steps taken to prevent grant fraud should be part of broader efforts to counter other types of fraud listed above. Some cases which look like possible grant fraud may be explained by honest mistakes or miscommunications, so developing an approach to grant fraud should take into account the relationships and communications channels that the foundation has with its grantees and applicants, and ensure they are robust enough to mitigate these risks.

There are two places in the grant making process where grant fraud can occur. The first is at the pre-award stage, when a person or organisation dishonestly misleads the foundation in the application process, either by not telling the whole truth (omission) or by telling a lie (commission). It is better to prevent fraud than to investigate it, therefore, we have concentrated on controls that help protect your funds in line with your risk appetite. The kinds of fraud that might occur at pre-award stage are detailed in examples A and B below.

Secondly, grant fraud can occur post-award, when a person or organisation deliberately uses grant money for purposes other than for which it was provided. This can be aggravated by the production of false accounts or false supporting evidence, but can be mitigated in the event that objectives were not clearly communicated. See examples C and D.

One way to prevent fraud is to make sure that terms and conditions are clearly set out and it is easy for grant recipients to report changes and ask questions. See example E.

[4] Crowe (2017) *Annual fraud indicator*: https://bit.ly/Crowe-indicator2017

Example A – Duplicate funding

Organisation A applies to your foundation to fund a project, the total cost of which is £5,000. Organisation A also applies to three other foundations who might provide funding.

Your foundation agrees to fund the full cost of the project. The other three foundations also agree to fund the full cost of the project.

Whether Organisation A has done anything wrong depends on whether they have been deceptive. If your foundation has asked in the application process if they are applying to other organisations and they say no, this is deceptive.

If your application process does *not* ask whether funding has been applied for from other sources, then the actions of Organisation A may not be dishonest. Speak to the applicant about its plans.

Example B – Bogus organisation

Organisation B approaches your foundation for a grant to deliver a project to engage young people in music and dance. They are not a legal entity, but a 'collective' who wish to share enjoyment of music and dance. In support of their application, Organisation B submit photos of an event, some governance documents and a referee at the local authority.

You check the internet and find that the collective has no website. You search the internet for the photo that was supplied in support of the application and find that it was taken at an unrelated event. You also find the governance documents are generic and freely available on the web. You call the contact at the local authority, but the number does not work.

This application would appear to be dishonest. Your foundation should have a process in place to manage this type of application.

Example C – False invoices

Your foundation has funded Organisation C to provide a project to fund a small event for young people. Organisation C provides evidence that the event has taken place by supplying invoices from suppliers of various equipment and photos of the day.

Your foundation receives a phone call from an anonymous caller stating that the event did not take place and that suppliers have not been paid. You take a closer look at the photos and find that they were not taken on the day or at the location which was claimed. You contact the companies that state they have supplied invoices and they tell you that they have not supplied the goods and services detailed.

This is dishonest activity and the foundation should have procedures in place to deal with such scenarios, in line with the charity regulators' guidelines.

Example D – Change of plans

Organisation D has been funded to provide a project for young people. Organisation D realises that it cannot attract the number of people they had said in their original application. They call your foundation and say that the project won't run as they had stated in their application.

This is not fraud, unless there is some form of dishonest behaviour. It is important that grantees feel they can contact your foundation to discuss potential problems with delivery.

Example E – Budget

Organisation E has completed the project, and you are happy with the outcome, but they have only spent £5,000 of the £7,000 grant. It creates false invoices for sundry expenses to cover the remaining money and submits them to your foundation. The left-over money is taken by the chairman and treasurer.

By creating false invoices to deceive the foundation this type of action is fraudulent. However, how budget underspends are managed is an area that grantees should feel comfortable discussing with your foundation.

Whose responsibility is tackling grant fraud?

It is likely that most of this guide will be implemented by staff within foundations, as it relates to assessing applicants, carrying out due diligence, and communicating with grantees. However, it is an essential trustee duty to manage the foundation's resources responsibly. This includes managing the risks that arise from grant fraud. Trustees are also vital in establishing a counter-fraud culture throughout the organisation [5].

What can trustees do to help minimise the risk of grant fraud?

Many trustees will be not be involved in day-to-day grants management and may not have relationships with individual recipient organisations. However, if a foundation is to implement an effective counter-fraud culture, it is important that the trustee board sets an appropriate tone about the foundation's counter-fraud stance. One way to do this is by developing a counter-fraud policy. For foundations in England and Wales the Charity Commission has guidance[6], OSCR has information for foundations in Scotland[7], and general advice is also is available on the Charities Fraud Awareness Hub[8].

[5] The Charity Commission for England and Wales defines a counter fraud culture as one that 'encourage[s] the robust use of fraud prevention controls and a willingness to challenge unusual activities and behaviour' http://bit.ly/CC-Fraud

[6] Templates for counter-fraud policies are available here: http://bit.ly/CC-Fraud

[7] OSCR (2018) *Fraud: how to reduce the risks in your charity*: https://bit.ly/OSCR-antifraudstrategy

[8] Charity Fraud Awareness Hub: http://bit.ly/FAP-CFAW19

If your organisation has not specifically considered the risk of grant fraud before, this might start with a discussion about the trustees' attitude to risk, often referred to as risk appetite[9]. Some will feel that taking measured risks with grant-making is entirely appropriate, that the very role of foundations is to fund those projects or organisations that other funders would not or could not support, while others will be more risk-averse.

This balance is a matter of choice for the individual foundation concerned. Some of the factors which may influence this include:

- The aims of the foundation
- The nature and areas of benefit of funding
- The type of organisations/individuals supported by the foundation
- The size of grants given
- The offer of any other kinds of support, e.g. funder plus, peer networking
- The level of staff resources which can be dedicated to monitoring a grant
- The geographical area served.

Once you have considered an appropriate level of risk for your foundation, a counter-fraud policy and a fraud response plan can be developed [10].

All trustees carry equal responsibility for the actions of the trustee board. However, for clarity, it may be useful to designate a trustee with responsibility for counter-fraud issues. This trustee could work with the executive staff on the production of a counter-fraud strategy, and would normally be involved in the instance of fraud being discovered. Mechanisms should be put in place to ensure that any specialist knowledge that this trustee develops is not lost if that person stops being a trustee.

Whilst it will never be possible for a foundation to rule out completely the possibility of grant fraud, existing due diligence checks and the adoption of some of the mechanisms and approaches suggested in the rest of this guidance should help organisations to protect themselves.

[9] Risk appetite is defined by the Institute of Risk Management as "…the amount of risk that an organisation is willing to seek or accept in the pursuit of its long term objectives" https://bit.ly/IRM-riskappetite

[10] A fraud response plan recognises that your organisation may need to investigate an allegation of fraud, and sets out who will assume responsibility for each area including undertaking the investigation, reporting to relevant parties (e.g. trustees, beneficiaries, regulators), as well as who will manage communication plans and police reports as needed. A template is available here: https://bit.ly/BC-investigationtemplate

2. DUE DILIGENCE

Undertaking appropriate due diligence is an essential part of the grant-making process. However, even basic checks such as verifying the identity of an applicant can be a significant challenge, especially for foundations processing large numbers of applications or covering wide geographical areas. One useful phrase in due diligence might be 'politely sceptical', reminding staff that processes should be followed even though the grant recipient is trusted.

Verifying identities is an important consideration in the context of due diligence. It is important to undertake checks even when a charity registration number is provided to ensure that the organisation applying for funds is aware of the actions of an individual. It is also important to trust grant recipients to use funds responsibly, and that processes are user-friendly for grantees. The balance between controls and simple processes will depend on the foundation's agreed risk appetite.

Verifying the identity of individuals

The Fraud Advisory Panel[11] recommends verifying the identities and assessing the fraud risks of all individuals listed in the grant application.

Foundations funding individuals are familiar with verifying that their applicants are genuine. Some ways in which foundations might do this include:

- **Carrying out face-to-face interviews** – either as a matter of course, or in cases identified as 'high risk'.
- **Asking referral agencies (such as statutory bodies) to verify the identity of the applican**t – this is particularly useful where the foundation covers a large geographical area, making it difficult to carry out interviews with individuals.
- **Requesting details for an independent referee from an approved list of contacts** – this should then either be followed up in writing, by email or by letter. If the reference is by email and is given based on the referee's professional relationship with an individual then it should come from the referee's business/official email address (personal references may come from unverifiable addresses). If the referee provides a reference by post then headed paper and/or an official stamp should be requested. Telephone references can be useful as referees can be more candid. It is important that you are sure that you are speaking to the referee; this can be aided by checking the phone number on the web.
- **Asking to see originals of specific official documents** – for example, passport, driving licence, or birth certificate.
- **Using a digital verification solution**
- **Verifying online presence**, e.g. LinkedIn, Twitter, etc.

[11] https://www.fraudadvisorypanel.org/

The Association of Charitable Organisations (ACO) has a guide to helping individuals in need that offers more factors to consider for those funding individuals[12].

Verifying the identity of organisations

Checking organisations on the regulators' register can provide assurance of the organisation's registration and details. Where the applicant is also a company, Companies House holds information on company directors, registered addresses and the company purposes. In addition, they hold filing information for all registered companies[13].

It is advisable not to store signatures on documents online. To include signatures can offer fraudsters the opportunity to impersonate the representatives of an organisation, including the organisation's cheque signatories. To combat this, charity regulators in certain cases accept unsigned copies of accounts, redacted versions, or typed signatures. Check with your relevant regulator for details.

Referees

Practice on whether to obtain independent references for applicant organisations is varied. Some foundations have stopped asking for references, feeling that they are an unreliable verification of another organisation and its work. Instead, they tend to speak to local contacts and rely on other forms of verification and support about an applicant's ability to deliver a project. Conversely, others have tightened up their requirements in this area.

Spot checks

A less formal way to verify the identity of an organisation is by speaking to the chair of the board or to the trustees. Some foundations will carry out 'spot checks' on applicants as part of their due diligence, or in cases where more information is needed. These may be undertaken by telephone or by visiting an applicant in person, if feasible. In order to do this, you will need to have legitimately obtained a phone number or an address, but where possible, this can be an easy and quick way to find out more about an applicant.

Online tools

There are a number of online tools that can help to verify whether an organisation is legitimate. For example, 360Giving[14] – an organisation which supports grant-makers to publish their grants data in an open standardised format – has a platform called GrantNav[15], which allows foundations to search for an organisation and see whether other funders have awarded it a grant. 360Giving does not capture all grants data as it is voluntary for funders to publish in this way, but it can be a useful starting point to see whether foundations or public bodies have made grants to an applicant before.

[12] http://bit.ly/ACO-Individuals
[13] Search for directors, companies and their details here: https://beta.companieshouse.gov.uk/
[14] https://www.threesixtygiving.org/
[15] http://grantnav.threesixtygiving.org/

In addition, details of all registered charities in England and Wales are listed on the Charity Commission website[16], those in Scotland on OSCR's website[17] and in Northern Ireland on the CCNI website[18].

Many applicant organisations will also have their own web presence, which can help to verify their existence and key staff or documents. Some applicants may not have websites, but may have a social media presence or connections to their local infrastructure body. While the existence of a website does not in itself prove legitimacy, it is likely that bona fide charities will have their charity registration details, contact details, and information about their work and staff which will help you in verifying their identity. OSCR encourages charities to use a unique registration logo to link to their entry on the register[19].

Local networks and contacts

It is common for foundations to speak to each other about grantees or applicants that they may have encountered; foundations share knowledge and learning from their work, and are eager to share positive experiences of effective organisations or projects. However, where something has given cause for concern or suspicion, foundations need to ensure that what they share is honest, fair, and grounded in evidence. See Section 3 on sharing information.

It is also common practice for foundations to seek information on applicants from local councils for voluntary service, statutory agencies and other relevant bodies (see Section 3 on data protection).

Quality assurance systems, such as NCVO's Trusted Charity Mark[20] (formerly known as PQASSO), are another way to provide some assurances that an organisation has a certain level of experience and professionalism, and is genuine. Groups that have had health checks carried out by umbrella bodies will also be able to provide additional information to demonstrate their history, as well as their capacity to deliver a particular project.

Common Reporting Standard

Some foundations may have to collect further information on their grantees and verify their identities under the Common Reporting Standard (CRS). This international tax transparency regime came into force in 2016. CRS, agreed at OECD level, creates Automatic Exchange of Information (AEIO) between the tax authorities of participating jurisdictions. While it is aimed primarily at banks and financial management services, foundations are included within the regime if they fulfil certain conditions, and so may have to report information about their grant holders to HMRC. Foundations are considered financial institutions if they rely on investments for more than 50% of their income and where any of those investments are externally managed by a financial institution under a discretionary mandate. This means some endowed foundations are affected, albeit to differing extents (definitions under the regime apply differently to incorporated and unincorporated charities).

Organisations that fall under the scope of the regime carry out due diligence on the tax residency status of their 'account holders'. In the case of foundations affected, grantees are considered to be

[16] https://www.gov.uk/find-charity-information
[17] https://bit.ly/OSCR-register
[18] https://www.charitycommissionni.org.uk/charity-search
[19] https://bit.ly/OSCR-logo
[20] http://bit.ly/NCVO-TC

account holders. Where those grantees are registered charities, their charity number is accepted as confirmation that they are tax resident in the UK. Individuals and other organisations can self-certify, and it is for the foundation to decide whether this information can be reasonably relied upon before submitting to HMRC if necessary.

ACF produced resources to help foundations understand and implement their responsibilities under the Common Reporting Standard[21].

Disqualified trustees

All three UK charity regulators have clear guidance on what constitutes a disqualified trustee.

The Charity Commission for England and Wales updated its rules on trustee disqualification in 2018[22]. There is now a wider range of circumstances and offences that can trigger a disqualification, and the rules apply to senior managers as well as trustees, though individuals can apply for a waiver. The Commission suggests (but doesn't insist) that charities seek signed declarations from new and existing staff and trustees that they are not disqualified. Other relevant registers to check include:

- Insolvency Service Register[23] for England and Wales. See also Scotland's insolvency service[24] or Northern Ireland's insolvency service[25]
- Register of disqualified directors[26]
- Register of all persons who have been removed as a charity trustee in England and Wales[27]

Foundations may also wish to check Unlock's resources[28] on how the guidance affects those with criminal convictions.

Scottish charity law also disqualifies some individuals from being trustees, unless they have been granted a waiver[29]. Details can be found on OSCR's website alongside what constitutes grounds for disqualification and waivers.

The Charity Commission for Northern Ireland maintains a similar register of disqualified trustees and individuals can apply for a waiver there too[30].

[21] https://www.acf.org.uk/policy-practice/common-reporting-standard/
[22] https://bit.ly/CCEW-disqualification
[23] https://bit.ly/EW-insolvency
[24] https://roi.aib.gov.uk/roi
[25] https://bit.ly/NI-insolvency
[26] https://bit.ly/disqual-directors
[27] https://bit.ly/CCEW-removedtrustees
[28] https://bit.ly/Unlock-charityrules
[29] https://bit.ly/OSCR-goodpractice
[30] https://bit.ly/CCNI-disqualified

Guidance from other sectors

Government

Action Fraud is the national centre for reporting incidents of fraud to the police in England, Wales and Northern Ireland, as well as providing information for individuals and businesses to protect against fraud. It also offers free cybercrime protection[31] that will help stop you from visiting malicious websites and protect you from email fraud for home users and businesses. In Scotland, fraud should be reported to Police Scotland on 101.

Action Fraud is run by the City of London Police working alongside the National Fraud Intelligence Bureau. The following websites may be useful resources in enhancing your foundation's cybersecurity:

- **National Cyber Security Centre**[32] supports the most critical organisations in the UK, providing guidance for the wider public sector and industry as well as the general public. It also has specific resources for small charities[33]. When incidents do occur, the NCSC provides effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.
- **Protect your charity from fraud and cybercrime**[34], issued by the Charity Commission for England and Wales, has resources to support charities in enhancing their cybersecurity, including guiding principles and toolkits for boards.
- **Charity Fraud Awareness Hub**[35] is a one-stop shop for information on how to prevent, detect and respond to fraud committed against charities.
- **Take Five to Stop Fraud**[36] is a national campaign offering straightforward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate trusted organisations.

Financial services

The Joint Money Laundering Steering Group (JMLSG)[37] is a useful resource in helping to verify identities. JMLSG has guidance to reflect methods and changes in the landscape, most notably the EU Fifth Money Laundering Directive (5MLD) in January 2020. The 5MLD contributes to achieving the aims of the Financial Action Task Force (FATF), a global effort to combat money laundering and terrorist financing. Further information can be found the Financial Conduct Authority website[38].

[31] https://bit.ly/Quad9-DMARC
[32] https://www.ncsc.gov.uk/
[33] https://www.ncsc.gov.uk/charity
[34] http://bit.ly/CCEW-Protect
[35] http://bit.ly/FAP-CFAW19
[36] https://takefive-stopfraud.org.uk/
[37] https://bit.ly/JMLSG-guidance
[38] https://bit.ly/FCA-ML

3. SHARING INFORMATION

Sharing information about grant applicants can help to safeguard charitable funds so that it goes to the intended beneficiaries, and help prevent criminal activity. It is important that information is shared in accordance with the legal gateways that exist and do not breach data protection or freedom of information rules as this can adversely affect organisations or individuals and lead to large punitive fines from the Information Commissioner's Office (ICO) and/or prosecution.

Data Protection

The Data Protection Act 2018 replaced its 1998 predecessor and enshrined the European General Data Protection Regulations in UK law. The new regulations set high standards of data protection. Among the changes, the definitions of personal and sensitive data were expanded, the lawful bases for processing were strengthened, and individuals were granted further rights relating to their data.

ACF produced a comprehensive guide[39] to the GDPR for foundations, answering member questions on specific aspects of their practice.

One area to consider is how to share data with other foundations about applicants as part of their due diligence checks and to prevent and detect fraud. It is important to remember that the GDPR only applies to individuals' data and not organisations' data, so sharing information about an organisation does not fall under the scope of the GDPR. Where an individual at an organisation could be directly or indirectly identified – for example if the chief executive is named or referred to – this could class as personal data, and would have to be processed in accordance with the provisions in law.

If you make grants to individuals, you will almost certainly process personal data. Depending on the sort of data you process, and how you collect it (e.g. through a referral agency), you may need to make further provisions or take legal advice. For example, you may need to review what data is being collected and whether it is being used lawfully, or you may need to put in place an agreement with a referrals agency or any other third party that covers data protection and data sharing.

There are special exemptions in regard to sharing data for the prevention and detection of crime or in the event that legal action is going to be taken. These exemptions are most commonly exercised by law enforcement professionals, but can also be used by those conducting investigations on behalf of a charity.

Data protection statements

Application forms should include a data protection statement setting out how the foundation will use an individual's data and with whom it will be shared. You should also make it clear what the lawful

[39] http://bit.ly/ACF-GDPR

basis is for processing the data, obtain consent if necessary, and indicate where more information about your data protection policy and practice can be found.

Storing data

As well as highlighting the importance of storing data securely, the GDPR enhances standards on how long data might be stored for. It says that personal data should not be kept longer than it is needed. There are circumstances where there may be a legal duty to store data for a certain amount of time, for example for Gift Aid purposes, but when this isn't the case, the ICO encourages organisations to think about what is reasonable and conduct regular reviews.

Some foundations have commented that they keep personal data on record to ensure the same applicant isn't applying several times in a given period. While there might be a lawful basis to justify such an approach, it is important to ensure compliance with data protection regulations.

Sensitive data

Sensitive data, or special category data as it is known under the GDPR, requires further protections and provisions to other personal data. Special category data includes information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, or sexual orientation. There are strict conditions for processing this data; find out more on the ICO's website[40].

Freedom of Information Act / Freedom of Information (Scotland) Act

Freedom of Information (FOI) applies to information held by public authorities, either by requiring information to be published or allowing members of the public to request information. FOI won't apply to the majority of foundations, except where:

- You are a public authority (e.g. Lottery distributor, local authority)
- You are holding public authority data, for example as part of delivering a grant programme
- You routinely share your information with a public authority

If you are covered by FOI for one of these reasons, you should check your obligations and make sure any necessary procedures are in place. If you have any doubt as to whether you are acting in the capacity of a public authority, legal advice should be sought.

Defamation

There is the potential risk of a defamation claim if views and other information relating to the grant applicant are shared between grant funders, and that information is capable of defaming the applicant concerned. Information may be defamatory where it contains words that might lower the reputation

[40] https://bit.ly/ICO-special

of the applicant, expose the applicant to hatred, contempt or ridicule, or otherwise cause the applicant to be avoided, for example, by other grant-making bodies. As well as individual applicants, it is possible to defame charities, companies and partnerships.

The exchange of 'views' has to be treated with much more care than the exchange of factual information, as views and opinions fall into a grey area. Any personal views that are expressed should be honest, fair and reasonable, and expressed with just and proper cause.

Applicants are freely entitled to request to see the information that you are holding that relates to them, and to ask for what purpose you are holding that data and with whom you might share that data. This will include any views that are expressed, however personal, so care must be taken not to express private thoughts, however justified. Any views and information about potential applicants must therefore be based on fact and recorded accurately.

4. FINANCIAL DOCUMENTATION AND CHECKS

Pre-award

Statutory accounts

The most recent iteration of *Charity reporting and accounting: the essentials* is CC15d[41] in England and Wales. *A guide to charity accounts* is the relevant guidance in Scotland published by OSCR[42], and in Northern Ireland the regulator has published *Accounting and reporting essentials*[43].

Has the organisation provided a copy of the most recent accounts? If not, why not? Are the accounts the same as those that appear on the regulator's website? Are the accounts compliant with the latest Statement of Recommended Practice[44]? Has the auditor or independent examiner qualified the financial statements in any way?

It has been observed that some charities mistakenly declare that their accounts are 'qualified' when they are not. This is likely due to unfamiliarity with accounting terminology. If you see a set of accounts that are marked as qualified but seem not to have any issues, it is worth having a conversation with the applicant to understand their accounts and to raise awareness of this issue.

If you are funding a new or very small organisation which does not have to produce audited accounts, you can ask for copies of the most recent bank statements instead to verify the financial position.

Auditors and independent examiners

If the auditors/independent examiners are local to your foundation, are they known to you? Does the auditor/independent examiner appear to be independent from the organisation? For example, you might want to carry out further checks if they are based in the same premises as the applicant.

If you have doubts about the veracity of the accounts or the qualifications of those carrying out the audit, check the designatory letters that appear after the accountant's name and contact the relevant accountancy body. These can often be checked online.

Management accounts details

Consider asking for a copy of recent management accounts as these can provide an updated financial position. They also give an indication of day-to-day financial management.

[41] https://bit.ly/CCEW-cc15d
[42] https://bit.ly/OSCR-CharityAccounts
[43] https://bit.ly/CCNI-accounting
[44] https://bit.ly/charitySORP

Bank account

Ask for bank account name, number and sort code, as well as the name and position of signatories. These can be cross-referenced with the organisation's financial procedures to ensure that they are in accordance with stated requirements. Some charities, for a variety of reasons, may have issues opening and managing bank accounts, so it is important to understand where difficulties for applicants might arise, for example for smaller or international charities.

Where another organisation is able to accept grants on behalf of an applicant, a section should be included on the application form for the name, organisation and address of those receiving the funding. A name for the contact at this organisation should also be included. The organisation receiving funds into its account should be asked to sign a statement confirming that it has agreed to accept the grant, that it will pass the full amount onto the applicant and that it will account for the funding separately in its audited accounts.

Bank verification form / confirmation of bank account details

In their application packs, some foundations include pro-forma which asks for standard information about the applicant's bank account. Applicants are asked to provide verification from their bank that the account's details provided are correct. In some instances, confirmation is sought straight from the bank by the foundation.

Financial management

Does the organisation appear to be managing its finances effectively? Has there been a rapid increase or decrease in funding in the past year? If so, can this be explained satisfactorily?

Post-award

Financial controls

If you have a copy of the organisation's financial controls document, check how this works in practice. Are procedures being followed? If not, what is the explanation for this?

Proof of purchase

Where grants are given for equipment costs (e.g. a computer), a copy of the invoice might be requested. During a monitoring visit, the serial number on the invoice can be checked against that on the equipment which has been purchased.

Breakdown of budget

Check the budget provided at the end of the project against the grant offer details. Have all financial conditions been met? Has the organisation previously requested a variation in the way that the grant

is to be spent? If not, has the funding been spent as originally agreed? Be clear from the outset how the budget variations will be managed and the process for managing any underspend.

Receipts

Some foundations ask for originals receipts, some for copies, whilst others ask for a final breakdown of expenditure. Some foundations audit a sample of projects, as this can encourage all projects to keep receipts on the basis that they may be asked to provide them.

Audited accounts

Check the relevant accounts provided to see whether your grant has been acknowledged as requested. Are restricted grants classified as such in the accounts? Do the amounts tally with your own payment records? Is any of your grant award showing up in the organisation's reserves? If so, is it correctly classified?

Further considerations

Governance arrangements

In addition to the financial documentation checks listed above, you may also want to find out more about an applicant's governance arrangements. Some documentation may be available on the charity regulator's register and in the applicant's accounts, but foundations may also ask for a list of trustees (to ensure consistency with the register, where possible) as well as for copies of pertinent policies and procedures, for example around financial processes, to provide more information than is publicly available.

Grant funding an organisation that isn't a charity

Many foundations make grants to organisations that are not set up as UK charities; this might include social enterprises, community groups, or organisations based overseas. In 2016 the Charity Commission for England and Wales published guidance on this topic, which looks at the different considerations and risks when funding organisations that aren't registered charities[45].

Non-charities may produce accounts that are different to charity accounts, or not at all. Foundations should decide what due diligence will be undertaken in these circumstances, ensuring that appropriate procedures and governance arrangements are in place prior to granting an award.

Bank de-risking

One of the consequences of the global crackdown on money laundering and terrorist financing has been that many banks have become less willing to expose themselves to risk. As a result, some

[45] http://bit.ly/FundingNonCharities

charities, particularly those operating overseas and/or in conflict-affected areas, have experienced problems in opening or accessing bank accounts. While the regulators recommend that charities use mainstream regulated banking systems for all transactions, some may need to or prefer to use alternative methods to send payments overseas. If you have questions about an applicant's use of alternative payment methods, it is important to understand the context and how they assess and manage the risks involved. For more information, see Charity Finance Group's report on the impact of money laundering and counter-terrorism regulations on charities[46].

Making grant payments

Most foundations make grant payments in advance (i.e. at the start of the work), whereas other funders (like commissioners) pay in arrears. For grantees, payments in advance are helpful and often appreciated, but carry their own risks for the foundation. Splitting the grant payments into smaller, more frequent amounts is administratively burdensome, but can reduce risk and assist monitoring where there are concerns. Making payments contingent on financial documentation, visits or governance reviews can also be helpful in mitigating risk.

5. ELECTRONIC COMMUNICATIONS

Many foundations rely on online processes for their grant-making, from ensuring eligibility to receiving the application to offering a decision. It is possible, and in some cases preferable, for a grant-maker to conduct all interaction with an applicant digitally. It is vital that countering fraud is considered throughout the development and implementation of these processes.

We also see many foundations talking about the importance of building trust in funding relationships. This can include making visits to grantees, holding more conversations by phone or video call, and holding more face-to-face meetings. Building good relationships with grantees can help foster a counter-fraud culture, whereby organisations feel able to discuss issues with the foundation openly and honestly, whether they occur pre- or post-award

Whatever the overall approach, it is likely that foundations will rely on electronic communications for at least some parts of their processes and communications, and should embed a counter-fraud approach across them.

Emails, phishing and spear phishing

We will all be familiar with scam emails purportedly coming from financial service providers and other online service providers. Phishing emails that appear to come from charitable foundations tend to offer grants to recipients or sometimes job opportunities. The emails often ask the recipient to send personal or financial information by return. In other instances, they may contain a link to a document,

[46] https://bit.ly/CFG-money

perhaps on OneDrive or Dropbox, or an image that looks like an attachment. In fact, these emails include a disguised link which shows one URL or a name, but actually send you elsewhere or they refer you to a spoof webpage.

Because these scam emails can be generated and disseminated with relative ease by hackers, this type of deception is unlikely to diminish in the near future. Fortunately, most people are now alert to these fraud attempts, although fraudsters rely on the fact that someone will fall for their con. To limit any possible reputational damage, you are advised to act quickly if you believe your foundation's identity has been stolen in this way by contacting the webmail provider to report the theft of your identity by those transmitting the messages.

Your foundation could also consider including a webpage that outlines the kinds of information your organisation will and will not ask for to help prevent fraudsters using your charity's name to commit fraud.

Spear phishing is similar to phishing, but targeted. Where phishing sees an email being sent to many users, spear phishing emails are sent to one or few recipients and usually claim to be from a senior member of staff. For example, a member of a finance team may receive an 'urgent request' claiming to be from a chief executive to transfer funds immediately. Often the sender address will emulate the format of the organisation's email addresses. Given the small scale of the foundation community where many staff and trustees know one another, these phishing and spear phishing scams sometimes slip through when the recipient believes the email from the sender may be genuine.

Carelessness when sending emails can also pose a data protection risk. The Information Commissioner's Office[47] (ICO) found that email or post misdirection is to blame for around 10% of information security breaches in charities. Given the nature of the information that foundations often share both internally and externally, it is essential that staff and trustees are aware of this risk and take care when sending emails, and have appropriate procedures in place to address security breaches.

Websites and social media

Websites and social media provide useful platforms for foundations to publicise their work, invite applications, and communicate messages to a wide range of stakeholders. Foundations are also increasingly making more information available on their website, for example in publishing grants data or in setting out detailed guidance to assist prospective applicants.

Care should be taken when adding information to a website or social media page. For example, if the foundation wishes to use online portals for its grant-making or reporting, it is sensible to ensure they are password-protected and that information meant for grant-holders is only available to the intended recipients. Or when sharing photos on social media, ensure that there is no sensitive information inadvertently within view. Simple checks like these should form part of basic information security within your foundation.

Banking and other financial transactions are often carried out remotely, and many of the checks used by these institutions can also be transferred to grant-making. For example, as well as requiring

[47] https://bit.ly/ICO-trends

customers to set up passwords, many institutions issue security, authentication and/or verification codes for use during online transactions. The security code might be issued by email, with the authentication or verification code issued by post to a recognised address. Larger foundations may wish to consider adopting a similar practice for higher value grant schemes.

Cybercrime

Cybercrime comes in many forms. According to the Fraud Advisory Panel, there are two main types: cyber-dependent crimes, which are illicit intrusions into computer networks (this includes hacking and the disruption or downgrading of computer functionality and network space, such as malware and Denial of Service [DOS] or Distributed Denial of Service [DDOS] attacks); and cyber-enabled crimes which do not depend on computers or networks but have been transformed in scale or form by the use of the internet and communications technology. They fall into the following categories:

- Economic-related cybercrime, including:
    - Fraud
    - Intellectual property crime (e.g. piracy, counterfeiting and forgery)
- Online marketplaces for illegal items
- Malicious and offensive communications, including:
    - Communications sent via social media
    - Cyber bullying/trolling
    - Virtual mobbing
- Offences that specifically target individuals, including cyber-enabled violence against women and girls:
    - Disclosing private sexual images without consent
    - Cyber stalking and harassment
    - Coercion and control
- Child sexual offences and indecent images of children, including:
    - Child sexual abuse
    - Online grooming
    - Prohibited and indecent images of children
- Extreme pornography, obscene publications and prohibited images

Foundations are not exempt from cyber-dependent crimes like hacks or DDOS attacks. The National Cyber Security Centre's threat assessment of the UK charity sector gives a useful overview of the nature of cybercrime and the risks it poses to charities[48]. However, given the nature of foundation operations today, digital and cyber security must form integral parts of any counter-fraud approach.

The cloud

Cloud computing is becoming increasingly common in workplaces, with many foundations opting to store data and access web services this way. It has many security benefits, as the data is held separately from the foundation and is often subject to enhanced security measures. However, it is not

[48] https://bit.ly/NCSC-threat

entirely without risks, and some service providers offer better protection than others. See the National Cyber Security Centre's guidance on cloud security for more information[49].

Before purchasing a cloud-based customer relationship management (CRM) system, organisations should be content that it is secure from cyber-attacks, however, remember that most successful cyber-attacks are the result of a member of staff being duped rather than the system being hacked.

6. RESPONDING TO FRAUD

If you believe your foundation has been a victim of grant fraud, it is important to act quickly. Having a fraud response plan will help your foundation to do this. In addition, the Fraud Advisory Panel recommends the following actions:

- Inform your senior leadership (including any trustees that need to know)
- Ensure no money is paid out before you have looked into what is happening
- Report your concerns to the police, Action Fraud[50] (in England, Wales and Northern Ireland) or Police Scotland[51]
- Report the issues to your charity regulator as required.

Reporting serious incidents

Each charity regulator in the UK has a regime for reporting serious incidents or notifiable events. Trustees are expected to report incidents including fraud as soon as possible. Although the regulators may not be able to take action themselves – and you should report any criminal offences to the relevant authorities in addition – it is important to inform them to show that your foundation is well governed and effective in managing risks. Find out more about your regulator's requirements and expectations: Charity Commission for England and Wales, *How to report a serious incident in your charity*[52]*;* Scottish Charity Regulator, *Notifiable Events*[53]; Charity Commission for Northern Ireland *Serious incident reporting: A guide for charity trustees*[54]

The Charity Commission for England and Wales has also produced guidance on reporting serious incidents when they involve a partner organisation, with which foundations should be familiar[55]. ACF has produced a briefing note to help foundations interpret the guidance in their own contexts[56].

[49] https://bit.ly/NCSC-cloudsecurity
[50] https://www.actionfraud.police.uk/
[51] https://www.scotland.police.uk/
[52] http://bit.ly/SeriousIncidents
[53] https://bit.ly/OSCR-notifiable
[54] https://bit.ly/CCNI-serious
[55] http://bit.ly/CCEW-SIR
[56] http://bit.ly/ACF-SIR

7. CONTACTS AND USEFUL LINKS

Regulators and government

- Charity Commission for England and Wales
- Scottish Charity Regulator (OSCR)
- Charity Commission for Northern Ireland
- Companies House
- HM Treasury
- Information Commissioner's Office (ICO)

Charity support

- National Council for Voluntary Organisations (NCVO)
- Scottish Council for Voluntary Organisations (SCVO)
- Wales Council for Voluntary Action (WCVA)
- Northern Ireland Council for Voluntary Action (NICVA)
- Charity Finance Group (CFG)
- National Association of Voluntary and Community Action (NAVCA)

Fraud support

- Charity Fraud Awareness Hub
- Fraud Advisory Panel
- Fraud Women's Network
- London Fraud Forum
- North East Fraud Forum
- Protect your charity from fraud and cybercrime (from the Charity Commission for England Wales)
- Yorkshire and Humber Fraud Forum

Professional support

- Association of Accounting Technicians (AAT)
- Association of Certified Fraud Examiners (UK Chapter)
- Association of Charity Independent Examiners
- Chartered Institute of Management Accountants
- Chartered Institute of Public Finance and Accountancy
- CIFAS
- Institute of Chartered Accountants in England and Wales (ICAEW)
- Institute of Chartered Accountants in Ireland (ICAI)
- Institute of Chartered Accountants in Scotland (ICAS)
- Institute of Chartered Certified Accountants (ACCA)
- Institute of Risk Management

Further reading

Preventing charity fraud: insights and action [PDF]
Charity Commission for England and Wales and Fraud Advisory Panel (2019)

Tackling charity fraud: prevention is better than cure [PDF]
Charity Commission for England and Wales and Fraud Advisory Panel (2018)

An introduction to moving money safely [PDF]
Charity Commission for England and Wales and Fraud Advisory Panel (2018)

Fraud: how to reduce the risks in your charity [webpage]
OSCR (2018)

Guidance and good practice for Charity Trustees – Charity finances [webpage]
OSCR (2016)

Getting to know your grant holders [PDF]
Charity Commission for England and Wales and Fraud Advisory Panel (2018)

Charity Fraud Awareness Week [website]
Charity Commission for England and Wales (2018)

Internal financial controls for charities [guidance]
Charity Commission for England and Wales (2012)

Countering fraud: a guide for the UK charity sector [PDF]
Charity Finance Group (2016)

Fraud and the 3 Cs [blog]
Charity Finance Group (2017)

Risk assessment toolkit [website]
NCVO Knowhow (2018)

Cyber security: small charity guide [website]
National Cyber Security Centre, part of GCHQ (2018)

The grant-making tango: issues for funders [PDF]
Julia Unwin (2004)