Tackling External Grant Fraud: a guide to help charitable trusts and foundations deter and detect fraud

Edited online version, December 2008

Association of Charitable Foundations

Tackling External Grant Fraud:
a guide to help charitable trusts and foundations deter and detect fraud

Background

In March 2006, the Association of Charitable Foundations (ACF) set up a Grant Risk Management Project, following the exposure of a number of its members to suspected fraudulent applications. The Grant Risk Management Project aimed to raise awareness of the issue amongst member trusts and foundations and share and develop good practice in this area. The project was supported by a consortium of member trusts and led by a part-time project officer.

This document follows on from the ACF guidance *Minimising the Risk of External Grant Fraud* – an overview which was issued to ACF members in July 2006. It covers a number of the issues on which ACF members sought information during the course of ACF's Grant Risk Management Project. A hard copy has already been distributed to all members. This is an edited online version.

Who is this guidance for?

It is likely that most of the more detailed guidance included in this document will be used by operational staff within trusts. However, we begin with an introductory chapter for trustees, which sets out trustees' responsibilities in this area. This is because trustees are vital for setting an anti-fraud culture within an organisation, which should then permeate throughout.

Contents

Endorsements

"If your charity hasn't assessed fraud risks and taken actions to minimise them then it's a sitting duck. ACF's guidance covers everything you need to know, and do, to make sure your foundation can analyse its risks and is equipped to manage them practically and effectively. Complacency is the enemy – don't assume it couldn't happen to you."

Rosie Chapman, Executive Director, Policy & Effectiveness, Charity Commission

"The Fraud Advisory Panel (FAP) warmly supports the Association of Charitable Foundation's guidance in assessing the risk of fraud when considering grant-giving by charitable bodies. The risk of fraudsters targeting the charitable sector is now recognised as a very real one and one that should not be underestimated. The ACF's role in helping its members to learn from good practice and each other's experience will go a long way in identifying common ways in which fraudsters can and do attack charities. The guidance includes useful advice on the collection and use of confidential personal data and will dispel some of the myths around data-sharing between charitable bodies, for the purpose of avoiding fraud. The FAP is delighted to see that ACF includes sample fraud policies in its guidance for use by members. Fraud policies and their active implementation are key to good risk management in charitable organisations just as much as in commercial firms. This is an excellent initiative on the part of ACF."

Rosalind Wright CB QC, Chairman, Fraud Advisory Panel

Acknowledgements

The Grant Risk Management Project, including the production of this guidance, was made possible through the financial support of six ACF members. ACF is most grateful to these members for their support, to the excellent Steering Group for their advice throughout the project, and to all those who contributed in other ways.

This guidance was written for ACF by Melanie Griffiths, Grant Risk Management Project Officer.

It would be helpful to receive comments on the guidance and further examples of controls used by trusts to deter and detect fraud. It would also be useful to hear from you, in confidence, if you have experienced external grant fraud.

1. **Trustees:** an introduction

Although most of the more detailed guidance included in this document is aimed at those who assess grant applications, we start with an introductory chapter for trustees, setting out their responsibilities in this area. Trustees are vital for setting the risk appetite of a trust and establishing an anti-fraud culture, both of which should then be carried through the organisation.

Why is external grant fraud an issue? *"It's never happened to us"*

Like organisations in the financial services industry, grant-making charities – which exist to distribute funding – are obvious targets for fraudulent activity. ACF has found that, combined with an assumption that those working in the charitable sector are likely to be 'benign', this has left grant-making trusts vulnerable to external grant fraud. In late 2004, it emerged that fraudsters were targeting charitable trusts in an organised way, and recent cases reported to ACF suggest that this is still happening.

The scale of external grant fraud – both in terms of incidence and the amount concerned – is not currently known. Charitable trusts and foundations are not alone in this uncertainty. Following its inter-departmental Fraud Review in 2006, the Government's 2006 report recognised that it did not know the scale of fraud in the UK. In those sectors where fraud was recorded, the measurements used were not consistent with those used in other sectors, making comparisons difficult.

However, an independent study commissioned by the Association of Chief Police Officers' Economic Crime Portfolio Group found that fraud – including income tax and EU fraud – costs the United Kingdom £20 billion a year[1]. 18% of charities responding to accountancy firm PKF and the Charity Finance Directors Group's 2007 risk survey indicated that they had

1 *The Nature, Extent and Economic Impact of Fraud in the UK*, report for the Association of Chief Police Officers' Economic Crime Portfolio, February 2007

been victims of fraud in the previous two years, and 6% of organisations had been a victim more than once[2]. And this is likely to be a significant under-estimate of the actual position.

During the course of ACF's Grant Risk Management Project, we came across many members who had been targeted for relatively small sums of money from applicants. Fraudsters often hide behind the legitimacy that charity registration appears to give them, and continue to submit funding applications. Sometimes, the supposed projects for which they are seeking support run alongside genuine activity within an organisation, whilst, on other occasions, sham organisations have been uncovered.

We have also found a range of attitudes amongst member trusts towards external grant fraud. Whilst some feel that fraud could not happen to them, many more have tightened up their existing procedures and there is, generally, a higher awareness of the possibility of fraudulent action.

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

The revised SORP 2005 (Statement of Recommended Practice for Accounting by Charities) continued the requirement for charities to include a statement in their Trustees' Annual Report to confirm that:

> *"The major risks to which the charity is exposed, as identified by the trustees, have been reviewed and systems or procedures have been established to manage those risks."*

For a grant-making trust, one of the key risks is clearly its grant-giving. Yet, according to the 2007 PKF and Charity Finance Directors' Group risk survey, only 45% of grant-making and relief charities that responded have assessed fraud risks[3].

2 *Managing risk – protecting your assets,* PKF charities' risk survey 2007 in association with the Charity Finance Directors' Group, September 2007

3 PKF and Charity Finance Directors' Group, September 2007

As a charity trustee, you are responsible for agreeing an appropriate risk strategy for your organisation and its grant programmes. Previous guidance from ACF, *Assessing Grant-Making Risk,* issued in May 2002, gives details to help trusts agree the level of risk that they are prepared to take with their grant-giving. Copies of this guidance are available from ACF, email: acf@acf.org.uk.

The Charity Commission's website includes useful advice for charities and general guidance on risk management. The Commission's *Internal Financial Controls for Charities* is particularly helpful – see www.charitycommission.gov.uk/publications/cc8.asp. Further information and support is also available from the Charity Finance Directors' Group website – see www.cfdg.org.uk.

Many trustees will, quite rightly, be remote from the day-to-day operations of grant management and from relationships with individual recipient organisations. However, if a trust is to implement an effective anti-fraud strategy, it is important that the trustee body sets an appropriate tone about the trust's anti-fraud stance.

If your organisation has not specifically considered grant fraud risk before, this might start with a discussion about the trustees' attitude to risk. Some will feel that taking measured risks with grant-making is entirely appropriate, that the very role of trusts and foundations is to fund those projects that public funders would never support. Others will be more risk-averse, perhaps because they have a higher public profile, tending to fund what they feel are 'safer' projects. This balance is a matter of choice for the individual trust concerned. Some of the factors which may influence this include:

- The aims of the trust.
- The nature and areas of benefit of funding and the type of organisations/ individuals supported by the trust.
- The size of grants given.
- The level of staff resources which can be dedicated to monitoring a grant.
- The geographical area served.

Once you've considered an appropriate level of risk for your particular trust, an anti-fraud strategy and response plan can be developed – see the enclosed sample documents (Chapter 6) for some ideas.

All trustees carry equal responsibility for the actions of the trustee board. However, for clarity, it may be useful to designate a particular trustee with responsibility for anti-fraud issues. This trustee could work with the Director and other staff on the production of an anti-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 trust to completely rule out the possibility of external grant fraud, existing due diligence checks and the adoption of some of the mechanisms and approaches suggested in the rest of this guidance document should help organisations to protect themselves.

Reporting fraud and other serious incidents to the Charity Commission

If your charity has an income of over £25,000, it is a legal requirement that you report all serious incidents – including fraud and money laundering – to the Charity Commission as soon as possible after you become aware of them. If you have not done so during the year, then you must report such incidents as part of your Annual Return to the Commission. Further guidance on this is available from the Commission – see **www.charitycommission.gov.uk/Library/investigations/pdfs/rsinotes.pdf**

2. Verifying identities

Following on from the introductory chapter for trustees, the remainder of this document is likely to be of greater relevance to grants administrators. For the purpose of this document, we are using a broad definition of grants administrators in order to cover all staff (or indeed trustees) responsible for operational matters, including grants managers; any staff who interact with grants applicants; and those who carry out more detailed grant assessment work. We look here, initially, at the key issue of verifying the identities of grant applicants.

Chapter 2

Identity theft is a huge problem in the UK. For trusts, particularly those covering a larger geographic area, the issue of verifying identities of applicants can pose a real challenge. However, awareness of identity theft is rising, and there has been a great deal of work carried out by both charitable trusts and in other sectors to address this issue.

Although obvious, it's worth mentioning that if you know the key contacts within an organisation, and have seen the organisation 'in action', then you will be far more likely to be able to verify the identities of those involved. During the course of ACF's Grant Risk Management Project, many funders have commented on this and, in particular, on the importance of having some personal contact and developing a relationship with applicants. This might include visits to organisations, other meetings, face-to-face contact and/or telephone conversations, all of which can be particularly beneficial in helping to deter and detect fraudulent applications.

But what if this isn't possible? You may fund nationally but rely on a very small staff based in one area of the country to assess your applications. Or you may be assessing a high volume of applications for a funding programme that involves a rapid desk-based assessment process, and that doesn't allow the time or resources for visits.

The information gathered below from grant-making trusts, and from other sectors that have developed systems for tackling this problem, provides some suggestions on how to verify identities. Examples are also included for ways in which your trust might protect itself, and your employees and trustees, from identity theft.

The local newsagent or a faceless bank?

How is your trust viewed?

As part of the CIPFA-run Grant Fraud Awareness Course – currently part of ACF's Professional Development Programme – participants complete a short multiple-choice questionnaire. One of the questions asks whether you would return money to your local newsagent if they had given you too much change. Another question asks whether you would notify a bank if its cash machine was giving out too many notes. Consistently, more participants respond that they would be more likely to be honest with the local newsagent than the 'faceless' bank.

This suggests that applicants might be more inclined to be honest with a trust where time has been taken to establish a relationship and some personal contact has been made, so that the trust is not seen as 'faceless'.

Applicants – verifying the identity of individuals

Trusts funding individuals are used to having to verify that their applicants are actually who they say they are. Members of ACF's Giving to Individuals Issue Based Network have shared some of the ways in which they currently verify the identity of applicants. Examples include:

- Carrying out face-to-face interviews – either as a matter of course, or in cases identified as more 'high risk'.
- Asking referral agencies (such as statutory bodies) to verify the identity of the applicant – this is particularly useful where the trust covers a large geographical area, making it difficult to carry out interviews with individuals itself.

- Requesting details for an independent referee from an approved list of contacts – this should then either be followed up in writing, ensuring that the reference comes back on headed paper and/or with an official stamp, or by telephone to a specific number, for example, within a college or social services department.
- Asking to see originals of specific official documents – for example, passport, driving licence, birth certificate.

Referees

Practice on whether to obtain independent references for applicant organisations seems to have diversified in recent years. Some trusts have stopped asking for references, feeling that they are an unreliable external 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. Examples of these tighter requirements as used by individual trusts are available separately in hard copy for ACF members.

Dual identity

In Summer 2007, a national foundation contacted ACF with concerns about referees. The foundation had received two separate applications that appeared to have different referees – one was from a Counsellor, the other from a Pastor. However, grants staff had spotted that both referees had the same mobile phone number.

Grants Officers telephoned the 'two' referees a few hours apart. They spoke to the same man on both occasions, although during the second conversation he feigned ignorance about some of the areas covered during the first conversation, trying to maintain the illusion that he had not been contacted by the foundation staff previously.

The details of the two applicant organisations have been passed on to the police and the Charity Commission. One of the applicant organisations was already well known to the police.

Disqualified trustees

The Charity Commission keeps a register of disqualified trustees, which is available for inspection at the three Charity Commission offices in Liverpool, London and Taunton. Alternatively, to save the time and expense involved in visiting one of the offices, the Charity Commission has suggested that trusts ring the Commission's Contact Centre on 0845 3000 218. The Commission will carry out the checks for you and report back the findings. For further details see

www.charitycommission.gov.uk/supportingcharities/ogs/g041b003.asp

At the time of writing, the Office of the Scottish Charity Regulator (OSCR) was considering developing a list of disqualified trustees. For progress on this, trusts funding in Scotland should contact OSCR directly on 01382 220446.

Organisational identity

In recent years, Companies House has been required to tighten up the information that it stores on registered companies following major corporate identity fraud. Companies House now offers facilities for online filing, protected online filing and a monitoring service. For grant applicants that are registered companies, trusts can check basic details on the Companies House register free of charge – www.companieshouse.gov.uk.

Do not store signatures on documents online. To include such signatures can offer fraudsters the opportunity to impersonate the representatives of an organisation, including the organisation's cheque signatories. To combat this, the Charity Commission will now accept an unsigned copy of audited accounts which it will include in its publicly-available Register of Charities, provided this is followed up by a signed copy of the accounts for the Commission's own records. This development follows work undertaken by the Association of Charity Independent Examiners, which highlighted this problem to the Commission.

Local networks and contacts

It is common practice for trusts to seek information on applicants from Councils for Voluntary Service, other funders, statutory agencies and other relevant bodies – see Chapter 3 on Data Protection issues when sharing information.

Quality assurance systems, such as Charity Evaluation Service's PQASSO, and quality marks can also provide some assurances that an organisation has a track record, a certain level of experience and professionalism, and is who it claims to be. Similarly, groups that have had health checks carried out by umbrella bodies, such as those introduced by Voluntary Action Westminster and by Enfield Children & Young Persons' Services, will also be able to provide additional information to demonstrate their history, as well as their capacity to deliver a particular project.

Guidance from other sectors

- **The Financial Services Industry**

The Joint Money Laundering Steering Group (JMLSG) is made up of the leading UK Trade Associations in the Financial Services Industry, including the Association of British Insurers, British Bankers Association, and the Building Societies Association. The JMLSG's aim is *"to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations".*

JMLSG guidance suggests that there are two factors that need to be verified for an organisation to be reasonably satisfied that a customer is the person they claim to be. The two factors to be verified are:

1. Ensuring that **the named person exists** – by checking appropriate identity data and information; *and*
2. Ensuring that **the customer is that person** – by verifying from reliable, independent source documents, data or information, satisfactory confirmatory evidence of appropriate parts of the customer's accumulated profile.

Within the Financial Services Industry, there is a broad hierarchy of documents used for verification purposes, ranked as follows:

1. Certain documents issued by government departments and agencies or by a court – for example, passport, driving licence.
2. Certain documents issued by other public sector bodies or local authorities – for example, council tax demand or statement.
3. Certain documents issued by regulated firms in the financial services industry or others subject to comparable legislation – for example, bank or credit card statements.
4. Those issued by other organisations – for example, utility bills.

- **Other useful information sources outside the charity sector**

The **Home Office** website www.identitytheft.org.uk – includes useful information about what to do if you become a victim of identity crime, with practical information for victims. Although aimed at individuals, many of the protective measures suggested are equally transferable to organisations. For example,

- Keeping personal information safe.
- Keeping plastic cards safe.
- Keeping documents secure.
- Keeping passwords and PINs safe.
- Protecting the identity of deceased family members.

Business Link gives guidance on avoiding scams, provides helpful information for organisations trying to protect themselves against identity theft and other types of fraudulent activity – see www.businesslink.gov.uk

The Metropolitan Police's Operation Sterling has set up the Fraud Alert webpages. These include valuable explanations of many types of fraud including identity theft, advance fee fraud and money laundering – see www.met.police.uk/fraudalert/index.htm

CIFAS – the UK's Fraud Prevention Service includes useful information on identity fraud on its website – www.identityfraud.org.uk

Keesing Reference Systems provides a number of tools for checking identities, including Keesing Identity Checker, a manual which provides security features and other details of 300 identity documents from over 130 countries to allow authenticity of documents to be checked. Can be purchased from www.keesingref.com

3. **Sharing information:** Data Protection, the Freedom of Information Act and defamation

Sharing information about grant applicants can help to safeguard charitable funds, protect funding so that it goes to the intended beneficiaries (i.e., bona fide charities, voluntary organisations and individuals in need) and help prevent criminal activity. But how can information be shared without contravening Data Protection legislation and the Freedom of Information Act?

As part of the Grant Risk Management Project, ACF sought legal advice on this from Farrer & Co Solicitors, and this chapter summarises their response. A copy of the full advice from Farrer & Co is available to members from ACF on request. As always when considering legal issues, you are advised to seek independent advice to cover your own trust's particular needs.

The advice provided here includes detailed information about data protection principles and obligations. We start, however, with a sample data protection statement to give trusts an indication of the type of information that might be included on application forms.

A. **Data Protection statements**

In order to satisfy Data Protection obligations, application forms should routinely contain a Data Protection statement. **As a minimum it is recommended that such statements indicate:**

- What you intend to do with such data.
- Whether you intend to share the data with third parties, and, if so, who those third parties are and why you are sharing it with them.
- That by submitting the application form the individual gives his/her/the charity's consent to your processing of the data in accordance with the stated purpose(s).
- Where possible, for how long you will hold the data.

The following is a suggested statement that may be used:

"How your information will be used by [ABC Trust]:

As a necessary part of the application process [ABC Trust] will be collecting information about you, including personal data. ABC Trust obtains and uses such information as part of the process of assessing grant applications and for monitoring the use of those grants. From time to time ABC Trust will share the information with [other grant providers, trusts, and charities and external auditors] for the following purposes:

- *Determining, preventing or detecting crime.*
- *Ensuring that no one individual is receiving multiple grants.*
- *Validating any contract that we may enter into with you.*
- *As part of our external auditing requirements.*

We will not keep your information on file for longer than we need to. In usual circumstances your file will be shredded after [X] years.

By signing and submitting your application form you give your explicit consent for us to use data relating to you for the purposes outlined above".

In addition, it is often best practice to attach a short statement on any separate equal opportunities monitoring form, along the following lines:

"I agree and give my consent for the information used on this form to be processed by [ABC Trust] for the purpose of monitoring and promoting equal opportunities. I agree and acknowledge that this information may be retained, stored and processed by [ABC Trust] for this purpose."

B. **Data Protection Act**

General principles

The provisions of the Data Protection Act (the DPA) relate to personal data. Information about companies (or charities or voluntary organisations) is not personal and, accordingly, there are no requirements to protect this data. Also, a large proportion of company information, such as financial accounts, is available to the public.

However, a distinction needs to be drawn between information relating to a company, and information relating to an employee or director of that company. Information relating to an employee or director is personal data, and that individual has the same rights under the DPA as any other person as to how you process the data and how that data is stored. So, information held about XYZ Limited can be freely exchanged. Information about an employee of XYZ Limited is subject to the provisions of the DPA.

The DPA only applies to information which:

- Has a living individual as its focus.
- Is biographical in a significant sense.
- Affects an individual's privacy whether in his/her home life or professional life.

Sensitive personal data is more heavily regulated by the Act and generally requires explicit consent for processing. **Sensitive personal data is information which relates to a living individual's:**

- Race/ethnicity.
- Political opinions and religious beliefs.
- Trade union membership.
- Physical or mental health.
- Sexual life.
- Commission or alleged commission, or any criminal offence and related proceedings/sentence.

Funding for individuals or organisations?

If you are collecting information about individuals through your grant application form you are likely to be collecting personal data relating to that individual, i.e. information that makes it possible to identify the individual concerned. And some of the data is likely to include sensitive personal data – for example, information that relates to the individual's race or ethnicity. If you are collecting such data you must comply with certain legal obligations as to how you process that data and how you keep that data secure.

If you are providing funding to companies and/or unincorporated associations then, as a general rule, your obligations when sharing information about those companies/associations are less onerous than if you are funding individuals.

Processing data

For legal purposes 'processing data' can include any of the following acts:

- Organising, altering or adapting the data, for example, by creating a database that includes that data.
- Using the data.
- Sharing the data with third parties.

The principal obligations (or Data Protection Principles) are:

- Data must be processed fairly and lawfully.
- Data must only be obtained for one or more specified purposes.
- You must only collect as much data as is necessary for the specified purpose(s).
- All data held must be accurate and kept up-to-date, but should not be kept for longer than necessary.
- Measures should be taken to ensure the data is kept secure, to avoid any accidental loss or destruction.
- Data should not be transferred outside of Europe unless the country to which it will be transferred has an adequate level of data protection.

In addition to these obligations, an individual is entitled to request from you the following information:

- What data/information you are holding about him/her.
- For what purpose or purposes you are holding such data.
- With whom you might share that data.

Obtaining the consent of the individual before processing data

Before processing any personal data it is best practice to obtain the individual's consent to do so. However, consent is not necessarily required where:

- The processing of the data is necessary to assess whether to enter into a contract with the individual concerned, including providing funding or making a grant.
- The processing is necessary for the purposes of a legitimate interest, pursued by you or by third parties with whom you share the data. A legitimate interest may include the deterrence and detection of crime or fraud.

Extra obligations when holding sensitive personal data

Before processing sensitive personal data it is essential to obtain the explicit consent of the individual concerned before you share that sensitive personal data with any third party. There are exceptions where the explicit consent of the individual concerned may not be required, including where you are collecting information on race/ethnicity, for the purposes of monitoring and promoting equal opportunity.

Storing data

Care must be taken to store the data securely. You remain responsible, under this obligation, even if you outsource the storage and/or back-up of the data to a third party. Care must be taken to ensure appropriate safeguards are placed on the third party through the contract that you enter with them.

C. The Freedom of Information Act

The Freedom of Information Act (FOIA) will not affect most charitable trusts and foundations. However, if you are classified as a public authority, or you are likely to share data relating to the applicant with a public authority, you will also need to consider the impact of this Act.

Public authorities for the purpose of the FOIA include:

- Central government and government departments, including Lottery distribution bodies.
- Local authorities.
- State schools, colleges, universities and other education institutions.
- The police force and prison services.
- The National Health Service (hospitals, surgeries, dentists, pharmacies).

However, if you are not included above but you are carrying out a function on behalf of a public authority (for example, delivering a grant programme) and/or performing a task of public administration, then information that you hold relating to that function or task will be subject to the disclosure provisions of the FOIA. A company that is wholly owned by a public authority is also a public authority for the purposes of the FOIA.

If you have any doubt as to whether you are acting in the capacity of a public authority, legal advice should be sought.

Under the FOIA, a public authority may have to disclose data that it holds if a member of the public asks to see that data. The member of the public is entitled to be told whether the public authority holds the data requested and, if it does, the public authority may have to disclose it.

If you are a public authority or share information with a public authority you will be affected by these obligations, which may result in personal and sensitive personal data that you hold about an individual having to be disclosed. Consequently there are important additional legal considerations to consider – not least to ensure that you are still able to comply with the Data Protection Act.

A public authority is not under an absolute obligation to disclose such information. If the information falls into an exempt category then that information may not need to be disclosed. **The most relevant exemptions for trusts are:**

- The data is governed by the data protection principles outlined above; *and/or*
- The information is confidential; *and/or*
- The information is commercially sensitive.

Despite these exemptions a public authority is always required to consider whether there is a public interest in acceding to the information request. If there is a public interest, and this outweighs the exemptions, then the public authority must disclose the information under the provisions of the FOIA.

The FOIA and grant application forms

You will be under an obligation to make reference to the FOIA on the grant application form if:

- You are a public authority;
- You are delivering a grant programme on behalf of a public authority; or
- You routinely share your information with a public authority.

If this applies to you, you should inform the applicant that information they provide may have to be disclosed as part of your legal obligations under the FOIA. Accordingly a statement needs to be added to the general statement outlined on page 21. **Suggested wording is as follows:**

> *"We may be required to disclose information that we hold about you if required by law, including under the Freedom of Information Act 2000. If information is requested under The Freedom of Information Act we will release it subject to any exemptions that may apply."*

Public authorities – storing and sharing data

If you are a public authority that stores data or you share information with a public authority, it is recommended that a clear statement is attached to the document, database and/or forms containing the data, stating that you consider:

- That the document contains confidential and/or commercially sensitive data; and
- That such data is subject to the provisions of the Data Protection Act.

This should draw the attention of the public authority (or the officer who deals with FOIA requests) to the existence of the exemptions and set a marker: they should consider very carefully whether this information has to be disclosed to a third party under the FOIA.

Suggested wording which you might consider adding to any covering note is as follows:

"The information contained in the enclosed documents/forms is confidential and commercially sensitive and contains sensitive personal data as defined by the Data Protection Act. It is supplied to you for the purposes of your review only and must not be reproduced or used other than as agreed between us. The information should not be reproduced, disclosed or passed to any third party without our express prior written permission."

D. Sharing information – 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 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, rather than being clearly biased.

These principles apply equally to the full range of trusts in ACF's membership. However, it must be remembered that 'public bodies', for example, government-sponsored funding distribution bodies, are more likely to have to disclose information they hold under the FOIA.

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 factually-based and recorded accurately.

4. Financial documentation and checks

Checking appropriate financial documentation from applicants and grant recipients is one key way of verifying the activities undertaken by a funded organisation.

The tables below go through some of the different stages of the application process, and give examples of the types of financial documentation that some ACF members currently require at each stage. As with other information provided in this guidance, you and your colleagues will be best placed to decide whether using particular financial documents is appropriate for your trust or not.

Application and assessment	
Statutory accounts	For the most up-to-date information on accounting and reporting requirements, check the Charity Commission's guidance *Charity Reporting and Accounting: The Essentials* (CC15, www.charitycommission.gov.uk/publications/cc15.asp) [At the time of writing, the Charity Commission was updating its Operational Guidance. The new guidance will include advice about what to look for in a set of accounts, and will be a good source of reference when considering applications]. 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 Charity Commission website? Are the accounts compliant with the Statement of Recommended Practice 2005? Has the auditor or independent examiner qualified the financial statements in any way? If you are funding a new or very small organisation which does not have to produce audited accounts, 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 trust, 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 business 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 (see list provided in Chapter 8) and contact the relevant accountancy body.
Management accounts	Consider asking for a copy of recent management accounts as these can provide an updated financial position. They also give an indication of the day-to-day financial management of the organisation.
Bank account details	Ask for bank account name, account number and sort code, as well as the name and position of those able to sign cheques. Cheque signatories can be cross-referenced with the organisation's financial procedures to ensure that they tally with stated requirements. 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 and landline number 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 trusts now include a *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 trust. (It's worth noting, however, that for some banks the Head Office has withdrawn the facility for local branches to verify account details for fraud prevention reasons!) See Appendix 1 to this chapter for an example.
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?

Monitoring	
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 (for example, a computer), a copy of the invoice might be requested. During a monitoring visit, the serial number on the invoice can then be checked against that on the equipment which has been purchased.

End of grant	
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?
Receipts	There is a mixture of practice in this area. Some ACF members ask for originals of receipts, some for copies, whilst others ask for a final breakdown of expenditure instead. One ACF member stamps receipts with their trust's details to prevent the same receipt being used to claim a grant from another funder.
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 shown 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?

Appendix 1 – Bank or building society account details form

Section A (for completion by the applicant organisation)

This form is required from all organisations except for schools, health bodies, parish or town councils. **You must send us this form, completed and stamped, with your application. Guidance notes are overleaf.**

Name of Bank or building society you hold an account with

Account name (for example Jack and Jill pre-school)

Bank or building society account number

Sort code

Building society roll number

What postal address does the bank or building society have on record for this account?

Postcode

How many people have to sign each cheque or withdrawal from the account?

Date account was opened Day/Month/Year

Please give details of all the people who can sign cheques or withdrawals from this account. Continue on a separate sheet if necessary (which must be stamped by the bank or building society). If any of these signatories are related or live at the same address we will require written confirmation from the bank or building society that these signatories cannot authorise payments together.

Full name | Position in organisation | Date of birth | Signature

Home address (incl. postcode)

Postcode

Full name | Position in organisation | Date of birth | Signature

Home address (incl. postcode)

Postcode

We authorise the above bank or building society to verify the details given on this form. We understand that the bank or building society may make a charge for doing this and agree to accept that charge.

Section B (for completion by your bank or building society)

To: The Manager, Applicant's bank/building society: Please check the above details. If they are correct, stamp and complete the declaration below and return this form to the account holder for submission with their grant application for funding.

I confirm that the account named above exists and is active and that the details given are correct.

Name | Position in bank/buiding society | Date

Signed

Official bank/building society stamp
(please also record the bank/building society address if not on your official stamp)

☐ For banks or building societies that do not use an official bank stamp: **We do not use an official bank stamp and have attached confirmation of the bank or building society account in section A, in a form that is in line with our own internal procedures. Please tick this box and attach your bank or building society account verification.**

Appendix 2

The publication *Is it Seaworthy? Assessing and Funding the Capacity of Voluntary and Community Organisations*, produced by the Governance Hub, the Workforce Hub and ACF in September 2007, includes a useful checklist of prompts that funders can use when assessing the financial capacity of an organisation – see Area 2 at

www.ncvo-vol.org.uk/uploadedFiles/NCVO/Publications/Publications_Catalogue/Trustee_and_Governance/Is_it_Seaworthy_pdf.pdf

5. **Electronic communications:** online applications, internet fraud and email scams

Email, websites and online grant-making offer the potential to revolutionise the way in which trusts operate, opening up the possibility of speedier and more efficient decision and grant offer processes. If it suits your trust's requirements, the complete grant-giving process can now be carried out remotely, without you ever either meeting or speaking to your beneficiaries.

But along with the advantages that this electronic communication can bring, there are many challenges. How do you verify that the applicant is who they say they are? Can you be sure that hackers don't have access to confidential information about your organisation or grant applicants? How can you prevent fraudsters from using your trust's own identity for their personal gain?

Electronic communications and verifying identity

This is one area where lessons from other industries can be particularly valuable. Increasingly, banking and other financial transactions are 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 customers to set up passwords, many institutions now 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 trusts may wish to consider adopting a similar practice for higher value grant schemes.

More information on verifying identity is available from ACF for members only

Phishing and email scams

ACF is now contacted on a fairly regular basis by members that have had emails sent out in their name. According to Webopedia, phishing, as this is known, is *"the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft".*

Members will be familiar with similar scam emails purportedly coming from financial service providers, Pay-Pal and other online service providers. Phishing emails that appear to come from charitable trusts 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, the emails include a disguised link which shows one URL or a name, but actually sends you elsewhere, or else 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 electronic fraud attempts, although the hackers do 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 trust'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.

The Metropolitan Police Service website includes useful information on reporting phishing emails, including instructions on how to forward the emails – for further details see www.met.police.uk/fraudalert/internet_headers.htm#5.

You may also wish to notify one of the online phishing archive providers, such as www.millersmiles.co.uk.

More detailed information on phishing and other types of email deception can be found in the Fraud Advisory Panel's publications *Have you been scammed? Identifying Internet and Email Scams*, which can be downloaded from www.fraudadvisorypanel.org/newsite/PDFs/advice/Have_You_Been_Scammed_Jul04.pdf, and *Cybercrime – what every SME should know*, www.fraudadvisorypanel.org/newsite/PDFs/advice/Cybercrime%20what%20every%20SME%20should%20know.pdf.

Online warning about bogus emails

Recently one member contacted ACF about bogus emails being sent in the charity's name. In order to limit damage caused by the emails, the foundation included the following statement on the front page of its website:

WARNING: We have recently become aware of the circulation of emails purporting to come from the XX Foundation offering grants or part time paid employment working from home. The XX Foundation has not authorised or distributed any such job offers and never makes unsolicited offers of grant funding by email. Do not reply to these bogus emails and do not provide any personal or financial information in response to them.

6. Contacts and further resources

Organisations

Association of Certified Fraud Examiners (UK Chapter)

www.acfeuk.co.uk
Telephone: 0121 240 4666

Charity Commission

www.charity-commission.gov.uk
Register of Charities:
www.charity-commission.gov.uk/registeredcharities/first.asp
Inquiry Reports:
www.charity-commission.gov.uk/investigations/inquiryreports/inqreps.asp
Telephone: 0845 3000218

Charity Finance Directors' Group

www.cfdg.org.uk
Telephone: 0845 345 3192

CIFAS – the UK's Fraud Prevention Service

www.cifas.org.uk

Companies House

www.companieshouse.gov.uk
Telephone: 0870 3333636

Fraud Advisory Panel

www.fraudadvisorypanel.org
Telephone: 020 7920 8721

HM Treasury

www.hm-treasury.gov.uk
Telephone: 020 7270 4558

Information Commissioners' Office

www.ico.gov.uk
Telephone: 0845 6306060

Institute of Risk Management

www.theirm.org
Runs a Charities Special Interest Group. For further details contact Oliver Boyle, Chairman of the Special Interest Group – oliver.boyle@thomasmiller.com

National Association for Voluntary and Community Action

www.navca.org.uk
Telephone: 0114 2786636

Office of the Scottish Charity Regulator

www.oscr.org.uk

The Scottish Charity Register:
www.oscr.org.uk/TheRegister.stm

Inquiries into Charities:
www.oscr.org.uk/Inquiriesintocharities.stm
Telephone: 01382 220446

Fraud Forums

Eastern Fraud Forum

www.easternfraudforum.co.uk
Telephone: 01603 680966

East of Scotland Fraud Forum

www.eastofscotlandfraudforum.org.uk
Telephone: 0131 665 6786

Fraud Advisory Panel

www.fraudadvisorypanel.org
Telephone: 020 7920 8721

Fraud Women's Network

www.fraudwomensnetwork.com
Telephone: 07534 494779

London Fraud Forum

www.londonfraudforum.co.uk

North East Fraud Forum

www.northeastfraudforum.co.uk

North West Fraud Forum

www.northwestfraudforum.co.uk

South West Fraud Forum

www.southwestfraudforum.co.uk
Telephone: 01244 350303

Yorkshire and Humber Fraud Forum

www.yhff.co.uk
Telephone: 0113 245 5514

Professional Bodies for Accountants and Independent Examiners

Association of Accounting Technicians (AAT)

Designatory letters: MAAT or FMAAT
www.aat.org.uk
Telephone: 020 7397 3000

Association of Charity Independent Examiners

Designatory letters: FCIE, MCIE or LCIE
www.acie.org.uk
Telephone: 01302 828 338

Chartered Institute of Management Accountants (CIMA)

Designatory letters: ACMA or FCMA
www.cimaglobal.com
Telephone: 020 8849 2251

Chartered Institute of Public Finance and Accountancy

Designatory letters: CPFA
www.cipfa.org.uk
Telephone: 020 7543 5600

Institute of Chartered Accountants in England and Wales (ICAEW)

Designatory letters: ACA or FCA
www.icaew.co.uk
Telephone: 020 7920 8100

Institute of Chartered Accountants in Scotland (ICAS)

Designatory letters: CA
www.icas.org.uk
Telephone: 0131 347 0100

Institute of Chartered Accountants in Ireland (ICAI)

Designatory letters: ACA or FCA
www.icai.ie
Telephone: 020 7059 5000

Institute of Chartered Certified Accountants

Designatory letters: ACCA or FCCA
www.accaglobal.com
Telephone: 0141 582 2000

Further Resources: Reports & Publications

A Discussion Paper on Risk and Good Grantmaking

Diana Leat/Big Lottery Fund Research, Issue 17, August 2005

Assessing Grant-Making Risk

ACF Information Paper, May 2002

Charities & Risk Management

Charity Commission guidance, July 2007

Fighting Fraud: A Guide for SMEs (second edition)

Fraud Advisory Panel, February 2006

Fraud Review – Final Report

Attorney General's Office, June 2006

Have you been scammed? Identifying Internet and Email Scams

Fraud Advisory Panel, July 2004

Identity Theft: Do You Know the Signs?

Fraud Advisory Panel, July 2003

Is it Seaworthy? Assessing and Funding the Capacity of Voluntary and Community Organisations

ACF, Governance Hub and Workforce Hub, September 2007

Managing the Risk of Fraud: A Guide for Managers

HM Treasury, May 2003

Managing Risk – Protecting your Assets

PKF and Charity Finance Directors' Group, September 2007

The Nature, Extent and Economic Impact of Fraud in the UK

Report for the Association of Chief Police Officers' Economic Crime Portfolio, February 2007

Tackling External Fraud in Grant-Making: A Guide to Good Practice

National Audit Office/Department for Culture, Media and Sport, March 2006

ACF is a company limited by guarantee registered in England and Wales.

Company registration number: 5190466.

Registered office: Central House, 14 Upper Woburn Place, London WC1H 0AE.

Registered charity number: 1105412.

Tel: 020 7255 4499, Fax: 0207255 4496. Email acf@acf.org.uk Website: www.acf.org.uk