# Keeping your charity safe from financial crime

HSBC UK

# Foreword



I'd like to start by sharing my heartfelt thanks for everything that you do to support our local communities across the UK.

As charity trustees, you work tirelessly to improve our society, environment and quality of life. You navigate complex and challenging environments, whilst continuing to demonstrate the passion, dedication and selflessness that it takes to run a charitable organisation.

We know that every not-for-profit is different – from local clubs to global aid organisations – and we are proud to look after each and every one of you.

We understand that smaller charities may not have the resources and expertise that their larger counterparts have, often relying on support from friends and families. That's why we have produced a guide to help trustees of these charities understand their financial responsibilities and remain vigilant to the threat of cybercrime.

We have an important role to play in supporting you. We want to help protect you, and the wider financial system, by gaining a better understanding of who you are, how you work and who you work with.

As a trustee, we know that you take your responsibilities to protect your organisation seriously. We hope that this guide helps you to safeguard your charity and enables you to continue to thrive.

**Stuart Tait**
Head of Commercial Banking, HSBC UK



# 01.Your responsibilities

As a trustee, your job is to act as the 'custodian' of your charity. You will want to consider the charity's best interests and help manage it responsibly.

As a trustee, you are responsible for the management of the charity – a responsibility which is shared with your co-trustees.

The Charity Commission for England and Wales sets out the key responsibilities and duties of a trustee, which include:

- Ensuring your charity is carrying out its purposes for the public benefit.
- Complying with your charity's governing document and the law.
- Acting in your charity's best interests.
- Managing your charity's resources responsibly.
- Acting with reasonable care and skill.
- Ensuring your charity is accountable.

Part of a trustee's job is to regularly review and assess the risks that your charity faces. This helps you to manage these risks and ensure your charity continues to fulfil its goals.

Risks can come in many forms. This guide will help you understand the financial crime risk, specific to this sector.

In summary, a trustee should be able to demonstrate that he or she has:

- Taken reasonable steps to help prevent financial abuse or loss of the charity's funds.
- Ensured that robust financial controls and procedures are in place and are suitable for the size and scope of your charity.
- Acted responsibly, and in the interests of the charity, when dealing with incidents of crime.

As a trustee, having a clear view of all of the activities of your charity is important. This includes its finances. To do this you should consider raising concerns and asking difficult questions about the charity's income, outgoings, payments and accounts. This helps you to safeguard the integrity of your charity and serve the wider interests of your community.

## In summary

The Charity Commission for England and Wales outlines five key focus areas that charities should focus safeguarding efforts on:

1. Terrorism financing.
2. Due diligence, monitoring and verifying the end use of charitable funds.
3. Fraud and financial crime.
4. Holding, moving and receiving funds safely.
5. Protecting charities from abuse for extremist purposes.

# 02.Know your donors and beneficiaries

As a trustee, it is your responsibility to select donors, partners and beneficiaries carefully. This helps you manage potential reputational and financial crime risks.

Key things to consider when managing these risks are:

- Identify who you are dealing with and check they are appropriate for your charity.
- Be confident that the individuals or organisations you are working with can deliver what's expected of them.
- Watch out for unusual or suspicious activities.

**Donations from individuals**

Your charity may receive money from a number of people and through different fundraising methods.

Some of the money coming in could be relatively small amounts from one-off donations, such as coins collected in a box or supporters participating in a sponsored event. You are not expected to know who every single small donor is.

However, if your charity receives large donations, you should know the donor and be confident that the source of the money is legitimate.

**Donations from companies, institutions or governments**

Your charity may also receive donations from organisations. If so, it is necessary to find out more about how and why these donations are being made – and to keep a record of them.
The following questions can help you do this:

- What does this organisation do and are you happy to be associated with it?
- If the money is from a company, is it registered on the Companies House website and have the funds come from the account of the organisation?
- What is the trading name and registered address of the organisation?
- If the funds have come from a personal account, have you asked why?
- Is the donation an unusually large amount?
- Did you receive the funds via a complex banking or money transfer arrangement? If so, why was this arrangement necessary?
- If you know the donor, has the money come through an intermediary? If so, have you been able to confirm that there is no financial crime risk in this arrangement, including tax evasion?

By asking these questions you are able to:

- Assess risks to which your charity could be exposed to by accepting the donation.
- Make sure it is appropriate for your charity to accept the donation.
- Have reasonable assurance that the donation is not from an inappropriate or illegal source.
- Prove that you have acted in good faith.



# Keeping records of how funds are used will help protect you from being exposed to the risk of financial crime.

### Know your beneficiaries

As well as knowing who is donating to your charity, you should know where the money is going – your beneficiaries. Keeping records of how funds are used will help protect you from being exposed to potential financial crime risks.

There are a number of questions which can help you gain a clearer picture of your beneficiaries:

- What evidence and records do you maintain to demonstrate all funds are going to the intended recipient?
- How do you identify and select beneficiaries?
- Is this the first time you have sent money to a beneficiary? If so, have you done the right checks on their identity – and how they will use the funds?
- Does your charity provide financial assistance, services or support on the basis of a certain amount per beneficiary? If so, do you have a process in place to ensure funds are shared properly between the beneficiaries?
- Do you have an internal monitoring and auditing process through which volunteers or employees can track all funds distributed?

### Know your partners

It is also important to know who you are working with and who your partners are.

The key things you may want to consider are:

- If you operate through intermediaries, do they also receive funds from other charities? If so, are you sure there is no ‘double-funding’, particularly where contributions are being made to cover costs that are not easy to check?
- Do you have a clear audit trail that tracks all funds being sent to partners?
- Are new partners able to safely handle, log and distribute large amounts of money in a lawful, traceable manner?
- Are you collecting and checking documents which prove partners have used the funds your charity has sent in the way you intended?
- Can you confirm your partner uses a formal banking system, or do they use a regulated money transfer company to receive the money you send?
- Do you match the impact of a partner’s work against your charity’s goals to make sure they are relevant and the money is being used in the best way possible?

**Example:**

## Do the right checks

A health charity received a large, unsolicited donation from a local business woman.

The trustees wanted to be sure they understood why the donation was made, and from whom.

They designated one trustee to carry out further checks on the donor’s motives and connections to their charity.

The donor confirmed she had a family connection with the health condition being researched with the money raised.

The donation came from a UK bank account directly into the charity’s account.

Having done these checks, the trustees were happy they had confirmed the source and reason for the donation.

The designated trustee recorded their findings in the charity’s ‘significant donor’ log and confirmed the identity of the donor.

# 03.The key financial risks

Unfortunately, financial crime affects all types and sizes of organisation. Here are the most common types of financial crime to be aware of.

**Fraud and theft**

Sadly, charities can be abused by fraudsters posing as genuine donors or volunteers.

There are many types of fraud, and criminals' methods are constantly changing. For example, your charity may be targeted, by imposters, in person or through emails, phone calls, letters or websites.

Your charity could be the victim of fraud or your charity's name could be used to commit fraud. The Charity Commission for England and Wales has provided charities with a series of "guiding principles" to tackle charity fraud.

These principles include:

- Fraud will always happen – Simply being a charity is no defence.
- Fraud threats change constantly – Charities need to be able to adapt their defences quickly and appropriately.
- Prevention is (far) better than cure – It is far more cost-effective to prevent fraud than to investigate it and remedy the damage done.
- Trust is exploited by fraudsters – Charities rely on trust and goodwill; which fraudsters try to exploit.
- Discovering fraud is a good thing – The first step in fighting fraud is to find it. This requires charities to talk openly and honestly about fraud.
- Report every individual fraud – The timely reporting of fraud is fundamental to strengthening the resilience of individual charities and the wider sector.
- Anti-fraud responses should be proportionate to the charity's size, activities and fraud risks.
- Fighting fraud is a job for everyone – Trustees in particular should manage fraud risks actively to satisfy themselves that the necessary counter-fraud arrangements are in place.

**Money laundering**

Money laundering happens when criminals hide money gained from unlawful activities. It is the name given to the way they 'clean' the proceeds from crime to make this money look legitimate.

Often money laundering involves – moving funds between different accounts, people or investments. Moving the money many times over makes it harder to trace where it has come from. Eventually the funds appear to have come from legal, reputable sources. In the past, organisations which operated on a cash basis were most at risk because cash is hard to trace. Today, the ability to move money electronically has created additional ways to launder money.

Charities are vulnerable because they can be used to 'mask' illegal activity.

**Example:**

## Insider Fraud

A charity supporting young people who are homeless was defrauded over a seven-year period by the financial controller who was a trusted and well-liked member of the team.

The financial controller was responsible for managing the charity's finances and internal controls. They were an integral member of the senior management team and the wider organisation, providing direction and input into day-to-day operations and longer-term strategic thinking.

However, this trust was found to be misplaced when it was discovered that the financial controller had been forging signatures on charity cheques to pay for their mortgage and child's education. Suspicions were raised when the chief executive received a call from the charity's bank manager querying their signature on a cheque to a debt recovery agency – something they had no knowledge of. The matter was reported to the chair of the trustee board and a team of experts were called in to find out what had happened. In the meantime, the charity's bank manager had identified other cheques that had unusual signatures, including some that appeared to have been signed by a manager who was on leave. Eventually it was found that the financial controller had kept one of the charity's cheque books and used it exclusively to forge cheques. The financial controller was prosecuted and sentenced to two years in jail. Some of the money was recovered.

**What changed as a result?**

- The charity's financial controls and policies on fraud and whistleblowing were reviewed and updated.
- A new online payment system was introduced so that cheques are no longer required.
- Trustee committees were also restructured to include a more active audit and risk function.

Source: Prevent Charity Fraud



### Bribery and corruption

Bribery occurs when money, goods or other benefits are used to try to change the behaviour of the recipient in a way that is favourable to the giver.

There are real risks for charities if they are associated with bribery, in any way. As well as legal penalties, the potential damage to reputation can be severe, and can impact your ability to raise money in the future.

Fraudsters have been using the Covid-19 pandemic in attempts to defraud charities. One common fraud has seen fraudsters approach charities, claiming to be from a legitimate organisation and able to provide information that could be of assistance to local charities, such as a list of at-risk vulnerable people in the local community who may require support from the charity. The victim has to click on a link to get the information, which leads to a fake website or asks the victim to make a payment.

### Cybercrime

Technology is at the core of our everyday lives and it presents opportunities for businesses of all sizes. But it's also given criminals new tools for gaining access to information and funds. It's critical that you are up-to-speed on what criminals are doing and – more importantly – what you can do to minimise the likelihood of becoming the victim of these types of attacks.

The Charity Commission for England and Wales identifies a five-step cybercrime prevention checklist for completion by charity trustees, staff and volunteers:

1. Acknowledge the increasing threat from cybercrime and the harm it can cause.
2. Clarify responsibility for managing the risk of cybercrime.
3. Raise awareness of the cyberthreat and encourage trustees, staff and volunteers to raise concerns, especially regarding phishing attacks and malicious emails.
4. Report successful cyberattacks to the Board and to appropriate external regulators, including the police and Charity Commission.
5. Aim to be open and transparent when dealing with cybercrime, adopting a proactive approach that prioritises prevention arrangements.

**Example:**

## Responding to multiple cyberattacks

A charity was the subject of five successful malware attacks over a three-month period. This included Wannacry ransomware, which exploited vulnerabilities in older non-supported operating systems, and a crypto-virus that entered the charity network using a remote access route.

Cybercriminals attempted to extort 30 Bitcoins from the charity, valued at that time at £186,000. The charity did not pay out, but instead undertook forensic IT activities to quantify the damage and put in place arrangements to mitigate the harm caused.

It was found that server backups had also been compromised. Although staff pay and other charity activities were affected for a three-week period, no data breaches were identified.

Source: Prevent Charity Fraud

It's critical that you are up-to-speed on what criminals are doing and – more importantly – what you can do to minimise the likelihood of becoming the victim of these types of attacks.

**Example:**

## Email account hacked and attempted mandate fraud

A charity worker had their email account hacked. A subsequent email sent by a legitimate partner charity was diverted by the hacker, adjusted with new bank account information and then forwarded on to the charity worker as originally intended. The adjusted email now requested that the charity make a £7,000 grant payment to a new bank account, controlled by the hacker, rather than the legitimate account of the partner charity. This is a type of cyber enabled mandate fraud.

Fortunately, the charity worker was told that the email account had been hacked and had become suspicious of the email regarding change of bank details. The grantpayment was not made. Subsequent checks confirmed that the email had been fraudulently altered. The charity worker took immediate steps to enhance controls by strengthening passwords used and installing a new hard drive on the computer.

Source: Prevent Charity Fraud

**Example:**

## Phishing attack

A large medical funding charity suffered two phishing attacks in a short period of time after fraudsters gained access to the email accounts of four senior officers of that charity. This occurred after the senior officers clicked on links in a hoax email, entering passwords which then allowed fraudsters access to sensitive information.

The police were contacted after the phishing attack was discovered and the incident reported to the Charity Commission and Information Commissioner's Office. Thanks to the immediate action that was taken there was no financial loss.

The charity has since taken steps to be more open and transparent about security breaches, including listing the phishing attack in their Annual Report. The charity also introduced a staff awareness training programme and hired a cyber-security specialist.

Source: Prevent Charity Fraud



# 04.Putting effective controls in place

Reasonable steps, to make sure your charity's funds are not misused, include having appropriate controls in place.

There's no 'one size fits all' approach to the controls that charities can put in place. It depends on the size and type of charity you run. Here are some practical steps to consider:

- Ensure records of the charity's income and expenditure are kept, together with receipts, invoices and supporting documents.
- Records of domestic and international payments should have enough detail to show that funds have been transferred and spent as you intended.
- Use 'tiered authority' and signature levels for payments. If a large payment is to be made, it may be appropriate to have a senior person authorise it.
- Check bank accounts regularly and reconcile bank statements.
- Keep an audit trail of decisions made by trustees and other managers.
- Store records digitally wherever possible. Set up IT controls so only a small number of authorised people can access them. Ensure that information is stored safely to avoid theft or fraud.
- Make sure hard drives, laptops and other electronics are kept securely, and moved about safely, to avoid data and identity theft.
- Keep computer security up-to-date by using anti-virus software and firewall protection.
- Ensure trustees, staff and volunteers are kept up-to-date about the fraud risks that your charity faces.

Putting these types of controls in place won't remove all exposure to financial crime, but they can significantly reduce it.

These kinds of checks and balances are especially important if your charity relies on support from volunteers, so everyone knows how they should be handling charitable funds.

**Example:**

## Small charity

A small animal charity receives a lot of donations in cash and via card payments. It doubled in size over three years, so the trustees decided to review their
financial controls.

Following that review, they decided to implement a new banking mandate, with new internet banking authorisations, to give them greater control over the movement of funds. They also increased reconciliation of transactions on their bank account from monthly to weekly. Finally, they reduced the number of people with access to sensitive information on the charity's IT system, by deleting users who were no longer involved in the organisation's work.

"It is important that you raise suspicious or unclear activity in the meeting."

**Trustee meetings**

Trustee meetings are a crucial part of managing your charity responsibly – and being able to prove you are doing so.

During meetings, it is important to review your charity's finances and check that trustees are acting appropriately in their roles. You should be prepared to ask questions and look at all the details. This includes reviewing reports on the flow of funds in and out of your charity.

Here are some practical steps that you could consider:

- Examine the charity's financial records to look for anything unusual or inconsistent. By doing this, you may be able to see if the accounts have been tampered with.
- Ask how you can be sure funds have reached their intended destination. If money has been forwarded on, do you have documents to prove who has received it?
- Ask about a new or unusual transaction, partner or project and the risks they pose. Sometimes a 'one-size fits all' method of reporting is not suitable.

It is important that you raise suspicious or unclear activity in the meeting. If suspicions arise, we would recommend asking for a second opinion and, even if your charity is small, that you consider minuting every meeting.

By recording your questions and the answers given, you can show you were making reasonable enquiries about the finances of your charity. If something goes wrong, you can prove that your decision was made with the best intentions.

If trustees make a decision to do something which falls outside the charity's aims and objectives, then trustees should consider minuting the decision and the reasons behind it.

If you believe your charity has been the victim of a financial crime, you should report your concerns to the police. You should also report serious instances – including fraud, or theft – to the Charity Commission for England and Wales.



**Example:**

## Good practice case study

More and more charities of all sizes are taking proactive and innovative approaches to tackling fraud. These case studies showcase some of the things they are doing. By sharing this knowledge and their experiences more widely we hope to help improve fraud resilience within individual charities and across the sector as a whole..

The appointment of a new chief officer for a foodbank charity was an opportunity for fresh eyes to review its policies, procedures and practices. The result was a number of low-cost improvements to safeguard and expand the food bank's funding.

Financial controls were reviewed and some new processes introduced. The organisation now operates within an agreed budget monitored monthly. All financial transactions are overseen by the treasurer, chair and chief officer. Budget variations must be authorised by the trustees.

New campaigns have been launched: ‘change for change’ encourages supporters to fill an empty jam jar with small change and deposit it in the collection box.

A survey among volunteers revealed some particular concerns about the security of petty cash and the need to expand online fundraising. A new, lockable collections box is now wall-mounted in a public area in clear sight of staff, volunteers and clients. The treasurer acts as key-holder, empties the box weekly (at random times) and keeps a proper record of the cash donations. A petty cash float is no longer needed because expenses are now paid through online banking. Donors are encouraged to use direct debits and BACS, further reducing cash-handling.

A number of unauthorised withdrawals from the operational bank account prompted a decision to move all banking online. Banking details are still made public so donations can be received direct and free of bank charges but transactions are reviewed twice-weekly to enable suspicious withdrawals to be quickly identified and investigated. Any funds surplus to immediate operational needs are transferred to a deposit account which is also closely controlled.

Fundraising has been diversified. To reduce reliance on a single fundraising platform new profiles have been set up on a number of others. ‘Be a brick, buy a brick’ encourages them to buy a £10 brick in the ‘wall of gratitude’ or to donate in some other way to help fund the charity’s new ‘Food HQ’.

Taken together the changes have saved time, reduced cash handling risks and improved the confidence of volunteers. Increased donations have made the charity more financially secure and better able to provide sustained support to the 6,300 people (more than a third of them children) it helps feed. With the objective of reducing operating costs (and so being able to help more people) it has also set itself on the path towards purchasing its own premises.

Source: Prevent Charity Fraud



**Operating a charity’s bank accounts**

As a trustee, it is your responsibility to supervise your charity’s bank accounts. For smaller charities, it will probably make sense for you to do this personally. If you are the trustee of a larger charity, you may want to delegate day-to-day supervision and control to a member of staff.

Your charity’s governing document should clearly set out who is permitted to sign cheques, and to authorise the money your charity spends.

It is suggested that your charity’s bank accounts be reconciled at least once a month. This is an accounting process used to compare two sets of records. These checks ensure that the figures match, are accurate and the money leaving an account is equal to the money spent. Any accounts that do not match may be reviewed by a second person in order to be resolved. If this cannot be done then you need to ask why.

A list of all accounts should be kept and reviewed. Dormant accounts – those that are rarely or never used – should be closed.

It can be risky to allow anyone who isn’t working for your charity, or responsible for its governance, to open an account in the charity’s name.

As a trustee, you should either authorise, or have clear sight of, the opening or closing of any accounts.

Charity accounts and funds should not be used for any personal activity by trustees, volunteers or other members of staff.

**Example:**

## Spoofed Account Fraud

An accountant at a charity received a phone call from a male purporting to be from a high street bank. The fraudster’s number was ‘spoofed’ to resemble the bank’s phone number and the caller stated there had been attempts by a third party to access their account. The fraudster spent considerable time gaining the confidence of the accountant, even sending a plausible email that looked like it had come from the bank. The fraudster persuaded the accountant to download software which allowed the fraudster remote access to the charity’s bank accounts. The accountant was convinced to provide login details for a second bank account. The fraudster told the accountant that both accounts would be subject to “ghost transactions” to test their security and the money would not actually leave the accounts. However, this was a lie and a six figure sum was transferred to numerous fraudulent accounts.

Source: Prevent Charity Fraud

# 05. Financing operations overseas

## If your charity has operations overseas, these could include high-risk jurisdictions.

You need to be aware of the additional risks involved so you can manage them effectively. These include:

- The physical risks of people working in politically unstable countries. You have a responsibility to make sure your staff and volunteers are safe wherever you are operating. For example, a conflict could break out and put the people working with your charity in danger. You may also be operating in an area where disease is common. Do you have the right policies in place to best protect all those working with, and for, your charity?
- The risk of moving money across borders, which makes it more difficult to apply your standard controls in unfamiliar territories.
- The risk that moving funds overseas creates extra opportunities for the money to be diverted. Changing money into other currencies; exchanging cash into goods and back again; local corruption; a lack of formal banking systems, and unregulated customs and practices, can all mean that you lose sight of where your charity's money is going and how it is being used.
- The risk you could lose money if the local banking system collapses or the exchange rate falls.
- The risk of that money being handled by volunteers, without the right controls in place, could mean that you don't have a clear picture of how funds flow through your organisation.
- The risk that you cannot control how funds are used at their destination in a country, upset by civil unrest or terrorist activity.

**Example:**
An aid charity that historically focused on the UK started raising funds to help people in need overseas. The trustees knew this created additional risks, so they decided to put additional controls in place.

These included making it policy that the charity would not make any cash payments outside the UK, and that it would review the latest UK government travel safety guidelines before allowing volunteers to travel overseas.

### Extra steps you could take to manage these risks

Generally, it is safest to transfer money through this banking system. When you are using the banking system, your banking partner will need a clear description of the work being carried out. They will need information on where the money has come from, where it is going and how it is being transferred.

When thinking about your operations overseas, you need to ask questions about the banking system of the countries you are operating in. You should have a clear picture of the political and social situation of the



"Operating overseas creates new risks for trustees to consider."

countries you are working in, and ask whether you are comfortable with any risks involved.

**Terrorist financing**
There is a risk that charities can be used to move money for terrorist organisations.

The following factors can make a charity vulnerable to a terrorist organisation diverting funds for their own use:

- Serving communities that are in geographically remote locations or areas with poor infrastructure.
- Moving funds to, or through, high risk countries, which could lead to money being diverted before it reaches the intended recipients.
- Moving funds in cash, which is easy to conceal and to divert, rather than through the formal banking system of the country you are operating in.

**Sanctioned individuals, organisations and countries**
Some countries, organisations and individuals have sanctions against them.

If your donors or beneficiaries reside outside the UK, it is important to find out if they are on any sanctions lists.

When moving funds abroad, extra controls are needed to ensure they are spent appropriately.

If you do operate on an international basis, you also need to know about any sanctions against countries that your charity is planning to work with.

You can do these checks by carrying out a public search on sanctions lists, and by checking to see if there have been any press reports mentioning the country, organisation or individual.

The UK government provides an online register of current embargoes and sanctions. This includes restrictions on terrorist organisations. These lists are not always complete and should be used alongside paid vetting services, if you need further assurances.

See: **https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions**
There are also a number of software packages commercially available.

The UK Government provides further advice on how charities can manage risks when working internationally. Key points include:

- When working in politically unstable countries, you need to show that you have weighed up the benefits of working in another country against the potential harm. For example, you should be able to demonstrate key risks you are likely to face, and ways to mitigate these risks.
- Protect your charity's staff and beneficiaries: You need to run appropriate checks on anyone who will be working with vulnerable people, and implement procedures to safeguard their interests and rights.
- Traceability: It is important to be able to reassure the public that funds are going where they're meant to. For example, you should have clear audit trails stating how much money has been moved and where it has been moved to.



# Useful information

**Responsibilities of Trustees: Charity Commission for England and Wales – The Essential Trustee: What do you need to know, what do you need to do**
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866947/CC3_feb20.pdf

**Protecting Charities from Harm: Compliance Toolkit**
https://www.gov.uk/government/collections/protecting-charities-from-harm-compliance-toolkit

**Preventing Charity Cybercrime: Insights + Actions**
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840997/Web_CC_Cyber.pdf

**Current Trade Sanctions, including Arms Embargoes and other Restrictions**
https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions

**Transparency International UK – Fighting Corruption Worldwide**
https://www.transparency.org.uk/

**Tackling Charity Fraud – Eight Guiding Principles**
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/841056/8_Guiding_Principles_for_Tackling_Fraud__Final__Oct19.pdf

**The International Money Laundering Information Network**
www.imolin.org

**Charities: How to Manage Risks when Working Internationally**
https://www.gov.uk/guidance/charities-how-to-manage-risks-when-working-internationally

**Prevent Charity Fraud**
https://preventcharityfraud.org.uk/

**Case Studies of Insider Fraud in Charities**
https://www.gov.uk/government/case-studies/case-studies-of-insider-fraud-in-charities

**HSBC Fraud Hub**
https://www.business.hsbc.uk/en-gb/fraud-hub

**Modern Banking Guide**
This guide for charities, voluntary organisations, faith and community groups aims to outline some of the ways modern banking can help you run your organisation safely and efficiently.

https://www.business.hsbc.uk/-/media/media/uk/pdfs/campaigns/modern-banking-guide.pdf

**Visit: www.business.hsbc.uk**

If you have any questions, please call us on **03457 60 60 60***.
If you are calling from outside the UK please dial **+44 1226 260 878.**

If you have a speech or hearing impairment, you can call our textphone service on **03457 125563**. If you are calling from overseas, our textphone number is **+44 2070 882077**.

* We're open 8am to 8pm Monday-Friday and 8am to 2pm on Saturdays. To help us continually improve our service and in the interests of security we may monitor and/or record your call.



HSBC UK Bank plc. Registered in England and Wales number 09928412. Registered Office: 1 Centenary Square, Birmingham, B1 1HQ, United Kingdom. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under registration number 765112.

HSBC UK