How charity & non-profits can protect themselves against fraud.

pem.

Welcome.

Charity Fraud Awareness Week, taking place 27 November - 1 December, is the perfect time to think about how we can raise awareness of fraud and cybercrime, whilst sharing good practice.

Fraud awareness is not important only one week of the year. We encourage you to start the conversation and make sure trustees, staff and volunteers are up to date on how to stop charity fraud.

We have gathered a number of our recent articles that cover fraud, internal controls and cybercrime that you may find useful. There are also resources on the Prevent Charity Fraud website.

Charities at risk of 'underestimating' online fraud.

Article first published: January 2023

The Charity Commission has warned charities against the risk of online fraud. A survey in October 2022 found around one in eight charities (12%) had experienced cybercrime in the previous 12 months.

This follows earlier findings indicating that the pandemic prompted increasing numbers of charities to move to digital fundraising and operating, exposing them to the risk of cybercrime.

Most concerningly to the Charity Commission, the survey highlighted a potential lack of awareness of the risks facing charities online, with just over 24% having a formal policy in place to manage the risk.

Similarly, only around half (55%) of charities reported that cyber security was a fairly or very high priority in their organisation. The Charity Commission's new survey explored charities' experiences of online cyber-attacks.

It found that over half of charities (51%) held electronic records on their customers, while 37% enabled people to donate online. A greater digital footprint increases a charity's vulnerability.

The most common types of attacks experienced were phishing and impersonation (where others impersonate the organisation in emails or online). For both attacks personal data is often at risk, and both attacks can often be countered by awareness training and testing.

Charity Commission guidance is available to help trustees here. This includes links to the National Cyber Security Centre (NCSC) toolkit. to protect your charity from fraud and cybercrime.

Know your volunteer.

Article first published: 22 May 2023

A judgment of Shrewsbury Crown Court, at the start of May, jailed a woman for two years for stealing almost £39,000 from a church in the nine months from September 2018 to June 2019.

Despite being new to the congregation, Dowe took up the post of volunteer treasurer. With access to the church credit cards she was able to fund a lavish lifestyle which was only identified when officials at the church asked to see the accounts. The church made no checks prior to Dowe taking up the position.

During her trial at Shrewsbury Crown Court, Suzanne Francis prosecuting, said that Dowe had been jailed in 1991 for obtaining property by deception. She was also convicted for a complex fraud operation in Wolverhampton in 2010, which saw her jailed for 18 months.

This is an expensive reminder that not all volunteers have the best interests of the charity in mind when accepting posts.

Basic checks such as asking for a CV, a declaration from the volunteer and requesting references are a good start. Due to the nature of the position handling finance, the charity might request that the role comes with a basic DBS check. Basic DBS checks can be used for any position or purpose, and cost £18 for all applicants, including volunteers. A charity cannot run a check without the permission of the volunteer.

There is more guidance available on the government website on the disclosure and application process for volunteers. Although not relevant in this case, certain roles may require a higher level of check. More information about eligibility can be found in the DBS eligibility guidance. In particular, those working with children and vulnerable adults should have enhanced DBS checks suitable for their role.

Guidance on safeguarding for Charities and Trustees can be found on the Charity Commission website.

Cryptoassets & modern fundraising.

Article first published: 22 May 2023

The new guidance on internal controls issued by the Charity Commission in April 2023 includes some helpful guidance on cryptoassets, including what they are (cryptocurrencies and non-fungible tokens (NFTs)); and the risks that may be associated with them, such as volatility, potential for fraud, anonymity, ability to use them.

The guidance emphasises the legal duty of trustees to manage their charity's resources properly. Where that involves new products such as cryptoassets, trustees should make sure they have assessed the risks of holding such assets and the limitations of using them prior to accepting the donation.

Charity Commission guidance gives trustees discretion to make the difficult decision of whether to accept or refuse a donation, based solely in the best interests of the charity.

Further guidance is available on knowing your donor Charity Commission guidance.

Trustees may decide to develop a policy not to accept cryptoasset donations on considering:

- the risks around such new and volatile assets
- the potential for fraud
- the anonymity of the donor
- the lack of protection compared to traditional currencies or financial products (since cryptoassets are largely unregulated charities are very unlikely to have access to the Financial Services Compensation Scheme (FSCS) or the Financial Conduct Authority (FCA) if something goes wrong)
- the potential to get it wrong due to laws on cryptoassets varying between countries (for example cryptoassets are banned in some countries and other countries have complex regulatory requirements)
- the limited uses for the asset (for example in a retail setting)
- the expertise needed to management the risks.

However, if cryptoasset donations are accepted, Charity Commission guidance sets out that a charity should:

- adopt a policy on accepting, refusing and using cryptoassets, including how you make decisions about converting them to traditional currency
- ensure the platform you are using is compliant with UK regulations and registered with the FCA for anti-money laundering and counterterrorism as required, if your charity is receiving donations directly in its crpyto wallet
- keep accurate records of donations, storage and use
- make sure you follow HMRC's guidance on the taxation of cryptoassets
- remember that you cannot claim Gift Aid on any cryptoassets
- review the benefits to your charity of accepting cryptocurrency versus the risk
- regularly review your policies on them.

If your charity is currently considering their policy further advice on the risks of using cryptoassets can be found on the FCA website and FSCS advice on cryptoassets is available on the financial services compensation scheme website. Expert advice is recommended.

Understanding internal controls for charities and non-profits.

Article first published: 22 May 2023

Internal financial controls for charities (CC8) has long been the "go to" guidance on basic internal controls that the Charity Commission expect to be in place. This guidance was updated in April 2023 to reflect the increasing use of the internet for banking, donations and other transactions.

It covers alternative banking arrangements and cryptoassets to highlight areas where trustees may not be sure that they have addressed risks and questions that a 21st century charity may be addressing. (Some of the risks around cryptocurrency are explored at the start of this newsletter).

Funds transferred using alternative banking methods have recently been included in the annual return so additional questions around controls match that development.

The style of the checklist has changed to reflect key areas of control and supervision and should be logical for trustees and management to complete.

Although the questionnaire has yes/no responses to its questions, we would advise all charities to document why they are satisfied the response is a 'yes', and develop an action plan where there is a 'no' that is relevant to the activities of the charity.

If the charity has activities that the trustees do not feel are covered by the checklist or their current risk assessment, then they should be supplementing the questions for those areas.

The first section covers general principles for all charities – questions to establish how well trustees understand the financial controls in place and their duties. Questions focus on:

- understanding whether the controls are appropriate (requesting professional advice if unsure)
- understanding the charity's financial information and the methods of monitoring and keeping track of the reporting
- understanding whether controls are embedded in the organisation
- carrying out an annual review of the controls – internally or with the help of internal audit
- ensuring appropriate segregation between roles
- ensure that procedures are in place for reporting suspicious incidents.

The next section covers operational risks.

The key points here are around understanding whether there is sufficient training and knowledge of policies by trustees, staff and volunteers, including an understanding of:

- why the charity is at risk from financial crime
- what the rules are around hospitality, acceptance of donations, register of interests, managing conflicts
- how the charity controls access and storage of data.

Following the overview, there are some more detailed questions around internal financial controls for banking.

These cover how bank accounts are opened, reconciled and monitored.

Online banking

As a development from the previous CC8, there are questions relating to online banking around security of electronic devices, management of passwords (and PINs) and understanding who is approved to access passwords and PINs.

The income section works through challenging trustees and management to identify whether they have controls to manage the completeness and accuracy of income recognition from all sources, and the ongoing security of that asset:

- donations (including procedures around 'tainted charity donations')
- public collections and fundraising events
- received online and via card readers through the post
- donations of cryptoassets
- trading income
- legacies whether gift aid is claimed wherever possible.

The flow of the expenditure section is also updated to reflect the potentially increased levels of payment being made by individuals rather than through central purchasing and finance systems.

They are updated for services such as Google Pay and Apple Pay. For all methods where control over purchasing is effectively delegated to the individual, charities must be sure that clear policies are in place and have appropriate oversight as these delegated processes give increased scope for an individual to commit an unwary charity to action or spending without authorisation.

This section also includes questions around paying wages, salaries, expenses, grants and handling related party transactions. The key here is having clear policies in place around identifying and managing conflicts and subsequent related party payments that can be followed. Internal financial controls for assets and investments comes next with questions covering use of assets, registers and insurance. It also touches on GDPR controls and controls over the use of restricted funds and endowment, if your charity has those funds.

Investments is encapsulated by an understanding of Charities and investment matters: a guide for trustees CC14 trustee duties when investing charity funds.

Finally there are questions on:

- loans
- hospitality
- internal audit and audit committees

Trustees have a legal duty to manage their charity's resources responsibly, including implementing appropriate financial controls and managing risk. Increasingly, charity auditors, independent examiners and others will hold them to account and ask to see their assessment and understand that judgment. This demands more than a feeling, or a general assurance from those to whom financial controls have been delegated. The guidance accompanying the CC8 checklist recommends that charities that are required to have an external audit, should have an internal audit committee. This assessment of internal controls may be one of its tasks.

Cyber fraud - risks and responses.

Article first published: 10 August 2023

Following our Charity & Non-profit working lunch in July 2023 where we discussed fraud and cyber risk, we have put together some highlights from the session.

The Cyber Security Breaches Survey 2023 shows that focus on cyber defences has seen a consistent decline in the last few years. Potentially due to the economic pressures and uncertainties post Covid. However, email fraud remains one of the most common methods of attack.

- 56% of charities with income over £0.5m have experienced a cyber-attack or breach.
- 33% of charities have cyber insurance.
- 9% of charity reports covered cyber risk.
- 19% of charities are aware of the 10 steps guidance (for IT professionals).
- 16% of charities have formal incidence response plans.

How you can help your organisation

- Understand the data you hold and where you hold the data.
- Assess the threat from external and internal sources.
- Create some basic standards to address the threats.
- Consider your insurance and cyber risk insurance.
- Consider cyber security guidance for boards.
- Cyber security should be focussed addressing the risks the organisation faces.

"Unlimited spending on cyber security may still not be enough - it must be focussed and cost effective"

The highest risks for any organisation often come from staff and volunteers, by accident or thoughtlessness, and often a desire to be helpful, which is preyed upon by malicious hackers.

Unfortunately charities are as vulnerable as any organisation - cyber criminals do not discriminate. Trustees and managers cannot afford to be over confident.

Cyber Essentials

The Government has in place a Cyber Essentials programme that is renewable annually. The accreditation reflects the latest requirements and an extra 1 or 2 steps are added each year to help ensure that organisations remain protected.

Some of the ways organisations may be able to manage risk are set out below:

Malicious file execution

Organisations should have a policy regarding personal use of machines, the software that can be uploaded and back up procedures. Staff should be regularly reminded of, and tested on, the need to be alert for phishing emails.

Mobile phones & laptops

Lost devices are often the cause of reputational damage. Where personal devices are used, device management can protect organisational data with the ability to wipe data remotely.

Privilege escalation

Inappropriate use of admin rights passwords may mean that harmful software can run in the background. Where admin passwords are necessary they should be segregated from the passwords and logins used for other systems, particularly for email.

Physical access

Passcodes and keys provide physical security but these can still be breached by being too polite. Opening doors for unknown people entering your office can be a risk. Visible ID policies can help or just asking the question.

Anti-virus protection

All devices should have up to date anti-virus protection. Either purchased, or using the available free software. Commercial alternatives are preferred as they provide segregation from the other systems used.

Social media

How do you control what is written about you or your organisation, even incidentally. A birthday cake for the boss celebrated online may give away vital information. A social media policy is key for every organisation. The level of security and protection should be considerate to the types of data held and the risks. A response should be planned and practiced in case events do not go as expected.

If you have any questions about any of the matters raised in this newsletter, please speak to your PEM contact, or contact us through our website.

The Charities & non-profit team.

Kelly Bretherick
kbretherick@pem.co.uk

Nikki Loan
nloan@pem.co.uk

Kathryn Hebden
khebden@pem.co.uk

Michael Hewett
mhewett@pem.co.uk

Judith Pederzolli
jpederzolli@pem.co.uk

Gemma Baratte
gbaratte@pem.co.uk

Kate Millard
cmillard@pem.co.uk

Robert Plumbly
rplumbly@pem.co.uk

PEM
Salisbury House
Station Road
Cambridge CB1 2LA

t. 01223 728222
e. pem@pem.co.uk

pem.co.uk

KRESTON GLOBAL