Reducing the risks posed by Serious Organised Crime

A resource for Third Sector Organisations

2018

Contents

1. Relevance of this resource

Do you:

- Have staff?
- Work with a range of volunteers?
- Have or have access to funding?
- Have or have access to confidential personal information?
- Have physical assets such as equipment or housing stock?
- Have an IT system?

If you answered yes to any of the above questions, then serious organised crime groups may have an interest in exploiting your organisation. This resource can help you to identify, assess and manage a wide range of risks to your business, staff and people you support. It is designed to support existing risk management processes and aims to:

- Help voluntary sector managers and trustees understand and assess the risks posed to their organisation by Serious Organised Crime
- Help you take action to reduce those risks
- Highlight and share examples of good practice
- Share sources of information and support that are available.

The resource has been collaboratively developed by The Serious Organised Crime Taskforce and The Criminal Justice Voluntary Sector Forum. We would welcome feedback on how useful you have found it, and any areas where you feel it could be improved or further developed. Please send any feedback to cjvsf@ccpscotland.org.

2. What are the implications of Serious Organised Crime for Third Sector organisations?

What is Serious Organised Crime?

"Serious Organised Crime is crime which:

- involves more than one person;
- is organised, meaning that it involves control, planning and use of specialist resources;
- causes, or has the potential to cause, significant harm; and
- involves benefit to the individuals concerned, particularly financial gain."

Source: Scottish Government (2015) Scotland's Serious Organised Crime Strategy, Available at: http://www.gov.scot/Resource/0047/00479632.pdf

There are 164 Organised Crime Group's in Scotland and 3282 individuals recorded as being involved in Serious Organised Crime.

Serious Organised Crime (SOC) can cause significant harm to the wellbeing of individuals and families. They may be victims of a wide range of organised crime including, for example: child sexual exploitation and abuse, human trafficking and exploitation, identity fraud, cybercrime or being blackmailed or held to ransom. These activities can create serious impacts to people's health, confidence, finances, privacy and personal safety and security. In some instances, organised crime groups will target vulnerable individuals and families and exploit them by coercing them into criminal activity such as the sale of drugs or other illicit goods or organised theft. Often a family's breadwinner is targeted, with the expectation that their family will also play a part in supporting this activity. This can put a lot of pressure on the family, who may be unaware of the contribution that they are making to supporting SOC until it is too late and they suffer the consequences of their involvement.

SOC Groups will look to identify and exploit any opportunity to create wealth for themselves at the expense and misery of others and use legitimate organisations to launder their cash. With a turnover of £4.9 billion, the Third Sector is an appealing target for these Groups.

Further information about the activities, threats and risks associated with SOC can be found in Scotland's Serious Organised Crime Strategy.[1]

[1] Scottish Government (2015) *Scotland's Serious Organised Crime Strategy*, Edinburgh: Scottish Government. Available at: http://www.gov.scot/Resource/0047/00479632.pdf

3. What can Third Sector Organisations do to help tackle Serious Organised Crime?

Third Sector organisations can help to deter SOC and reduce the harm caused by SOC by:

- Helping to divert people from involvement in Serious Organised Crime and its products
- Promoting positive alternatives
- Protecting their own organisations from cyber threats and fraud
- Helping to identify and detect those involved in Serious Organised Crime
- Contributing to stronger, more resilient communities.

Here are some examples of how Third Sector Organisations in Scotland are contributing to diversion and to protecting their organisations, staff and service users from the harm caused by SOC.

Developing services that help to divert people at risk from involvement in Serious Organised Crime

Sacro's Another Way service provides one-to-one, non-judgemental support to women who are at risk of or involved in sex work in Edinburgh. This can include support with a range of issues, including healthcare, addictions, domestic abuse, housing and parenting. In 2013/14, over 70% of women who were referred to Another Way either decreased their involvement with sex work or exited from prostitution completely.

The Another Way service works in partnership with a range of agencies, including NHS Lothian's Harm Reduction Team, The Women's Clinic and Police Scotland. By working in partnership, the service is able to offer an outreach service and a place of safety for women. The service also enables women to anonymously report offences through the National Ugly Mug (NUM) scheme and has been awarded Star Status by the scheme for adhering to best practice. This scheme collates incident reports and warnings received about dangerous individuals. The information that is reported is then used to warn other sex workers and potentially save their lives.

Example of how a third sector org has protected itself from the risks posed by SOC

Through hard work, a charity was successful in fundraising in 2016-17. Their activity involves significant publication and marketing costs from their supplier of such services

In March 2017, the charity receives an email from 'Shooting Star Publications Ltd' their supplier, advising that their bank account details and sort code have changed. Enclosed is the latest invoice for £29,760.32

The charity finance team have recently reviewed and updated their SOC Prevention processes, which included significantly amending the process for making payments to suppliers who intimate changes to bank account details. Angela works for the charity finance team and is aware of the new process, which is;

(1) Make an 'Open Source' check on the internet of the new bank account sort code and account details to uncover the (a) Location of the bank and check against the location of the company, and (b) Whether there are any blogs or information available to suggest this communication may be a scam.

(2) Make a direct phone call to the supplier from information contained within the Charity's own records - not from information contained within the email received. Enquire over the veracity of the change of bank account details. If the change appears genuine, request that the supplier repeats the request but with details of the previous AND the new bank account details referenced.

(3) Take your actions to a senior member of the charity finance team to review your activity and if satisfied to authorise the change of bank account details on the charity systems.

(4) If the communication is deemed to be a scam - consider sharing this information as an 'Alert' with other partner groups who may also be affected. Notify your bank of this attempt of Bank Mandate Fraud.

Through Angela making checks outlined in their new SOC Prevention processes, it was established that the email from the supplier was fraudulent. By following the amended process, the charity avoided making a payment of £29,760.32 to the organised crime group actively involved in bank mandate fraud activity.

Assessing the risk from Serious Organised Crime

Section 4 provides a starting point for you and your colleagues to consider your organisation's own exposure to the risks posed by SOC and what can be done to address these.

Accessing further sources of information and support

Annex A contains a list of further sources of information and support that are available to assist organisations in relation to SOC.

4. Serious Organised Crime Checklists for third sector organisations

This section provides checklists for third sector organisations, to help senior managers and trustees to better understand and assess their organisation's exposure to the risks posed by Serious Organised Crime. You may find it helpful to work through the relevant checklists, engaging trustees and other staff members as appropriate. The questions are designed to prompt discussions about and consideration of the different risks and how you can reduce your organisation's exposure to these.

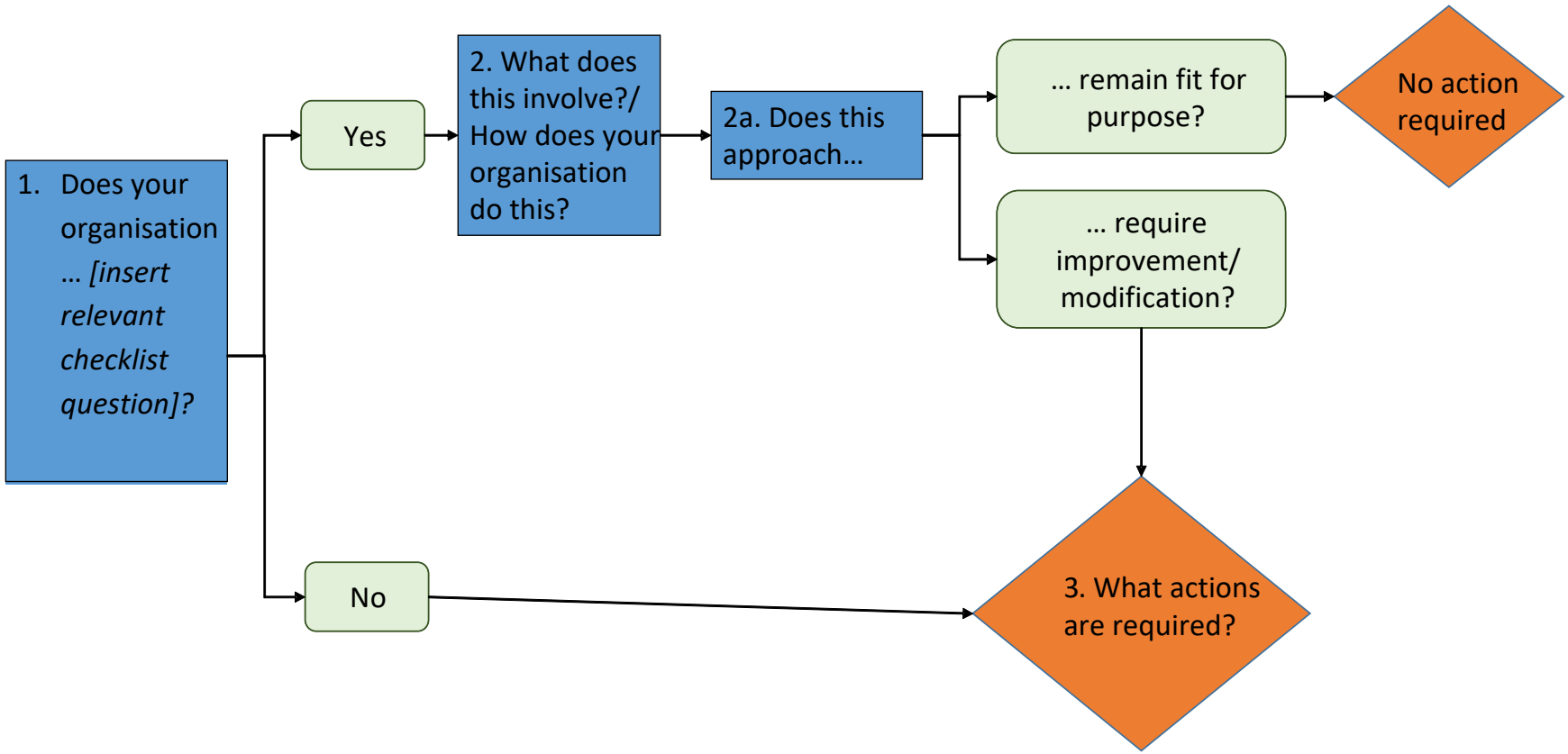
There are seven checklists, relating to issues and risks for:

1. People using your services
2. Staff and volunteers
3. Governance and threats to business continuity
4. Partner engagement
5. Fundraising
6. Commissioning and procurement
7. Physical assets.

The checklists are designed to cover most areas of operation within an organisation. It is recognised that you will already have in place processes and practices that identify, assess and mitigate risks. These checklists highlight some areas which you may not have considered as part of your organisation's internal self-evaluation and review processes. It is for each individual organisation to determine which elements may be of relevance to them, reviewing the element of risk against the benefits to be gained from any necessary or identified remedial action.

Each checklist contains questions for you to consider. We recommend the flow-chart overleaf be used to prompt discussion for each section and then record any identified actions.

Flowchart: Discussion prompt tool



1: People using your services

People using your services may be vulnerable to becoming victims of and/or becoming involved in Serious Organised Crime. Particular risk factors[2] include:

- *Criminality factors – offending patterns and trends;*
- *Ability – specialist skills, access or professional positions*
- *Networks – access to criminal associated through family, peer or professional networks; and*
- *Identity – upbringing and lifestyle factors.*

Possible issues to consider include:

- Physical or sexual violence, bullying, coercion, intimidation and psychological trauma
- Sexual exploitation and abuse
- Loss of money or other assets
- Involvement in crimes relating to drugs and substance misuse
- Involvement in other forms of SOC
- Modern slavery and human trafficking

Case study: Involvement of services users in drug related crime

Charity A runs an activity club at a local community centre in the evenings, popular with children and young people aged between 11 and 17. The attendees socialise, play games, and occasionally take part in organised activities. A local group involved in Serious Organised Crime has identified the evening sessions as a target for recruiting vulnerable young people to help them distribute drugs. The SOC group initially befriend a number of the attendees and, over time, bully and coerce a number of the young people to get involved in criminal activity, resulting in the community centre becoming a hub for local drug deals.

[2] As identified in The Serious and Organised Crime Interactive Toolkit: Home Office and partners (2015) *Serious and Organised Crime, An Interactive Toolkit for Practitioners working with Young People*. Available at: http://infed.org/mobi/soctoolkit/

Checklist 1: People using your services

Does your organisation:

- ☐ a) Identify people who may be at risk of *victimisation* of SOC?
- ☐ b) Identify people who may be at risk of *involvement* in SOC?
- ☐ c) Help people to access the support they need in relation to addressing the harm caused by SOC?

2: Staff and volunteers

Your staff and volunteers may be at risk of becoming victims of and/or becoming involved in Serious Organised Crime.

Possible issues to consider include:

- Bullying, coercion and intimidation
- Insider threats (considered under Section 3)
- The exploitation of staff or volunteers
- The personal circumstances of your staff and volunteers

Case study: Exploitation of volunteers

Charity B has a paid staff, and organises volunteers from vulnerable groups to provide a dog-walking service to isolated elderly people. Unbeknownst to the charity, a group involved in SOC is influencing one of the volunteers to get information about vulnerable people who can be targeted for doorstep crime, financial exploitation, fraud and burglaries. A number of the service users are victimised by the group, causing them substantial harm and financial loss. The police identify that the charity's service links the crimes, and trace it back to the individual volunteer. Though the charity is cleared of any wrongdoing, trust is lost and the organisation ceases to operate.

Checklist 2: Staff and volunteers

Does your organisation:

- ☐ a) Make your managers aware of the Scotland's Strategy for dealing with Serious Organised Crime?
- ☐ b) Embed the messages in the Strategy across the leadership of your organisation?
- ☐ c) Offer training to your staff and volunteers on the risks associated with organised crime?
- ☐ d) Have clear and effective whistle blowing/ confidential reporting arrangements in place?
- ☐ e) Have arrangements in place to protect and support staff and volunteers?

3: Governance and business continuity

Serious Organised Crime can also pose a risk to the operation of your organisation.

Possible issues to consider include:

- Fraud
- Corruption
- Insider threats
- Cybercrime

Case Study: Insider threats

Charity A provides a service where furniture is brought in to prison for refurbishment by inmates, as part of a training programme. A gang involved in organised crime has infiltrated the organisation, and is using the regular trips into the prison estate to smuggle drugs to prisoners. The impact of drugs entering the prison causes substantial harm to prisoners. The police are tipped off about the arrangement and conduct a raid on the charity's business premises, finding considerable amounts of drugs. Though ultimately found innocent of any wrongdoing, the matter causes huge reputational damage to the organisation, the loss of the key contract providing services to the prison, and ultimately leads to the closure of the charity.

Almost all organisations use computers in their business, be it for communication, business processes, or service delivery. SOC groups can be adept at exploiting IT vulnerabilities, as shown in the case study below.

Case Study: Cybercrime

Charity Y are a large national organisation who provide advocacy and support services for young people struggling to engage in education, working with schools and local authorities across Scotland. One day, the finance team receive an invoice seeking payment for a substantial sum in relation to IT services. The invoice is accompanied by a scanned receipt bearing the signature of the Chief Executive as confirmation. The finance officer carries out the instruction to pay the bank account detailed. A subsequent audit reveals that this claim was fraudulent, made by a criminal group involved in large scale financial fraud, who had taken the Chief Executive's signature from a published letter available on the charity's website. The charity suffers substantial financial loss.

Checklist 3: Governance and Business continuity

Does your organisation:

- [ ] a) Have up-to-date procedures in place to protect against fraud, corruption, insider threats and cybercrime?
- [ ] b) Have a risk register which includes the risks posed by SOC?
- [ ] c) Consider the risks posed by SOC from a Business Continuity perspective? i.e. How would your organisation respond to loss or harm caused by SOC?
- [ ] d) Report on your arrangements for managing and monitoring the risk of SOC
- [ ] e) Assess the risks to your organisation from employees or volunteers who may have links to SOC?
- [ ] f) Have a clear process for a member of staff, or another stakeholder to report suspected or alleged malpractice to you?

Checklist 3 (Cont'd)

Does your organisation:

- [ ] g) Have effective and up-to-date policies, procedures and agreed practices on vetting (on recruitment and thereafter)
- [ ] h) Have effective and up-to-date policies, procedures and agreed practices on gifts and hospitality (offered and received)
- [ ] i) Have effective and up-to-date policies, procedures and agreed practices on external interests (other employment, declarations of interest
- [ ] j) Have effective and up-to-date policies, procedures and agreed practices on (4) notifiable associations (e.g. associations with persons linked with crime)
- [ ] k) Have a way of identifying emerging threats, vulnerabilities, risk, opportunities and relevant mitigation measures to reduce the threat posed by SOC groups?
- [ ] l) Have effective and up-to-date policies, procedures and agreed practices on external interests (other employment, declarations of interest) (4) notifiable associations (e.g. associations with persons linked with crime)
- [ ] m) Have agreed minimum standards in relation to data security and online processes which mitigate the threat of cybercrime?
- [ ] n) Make your staff and volunteers aware of the risks of cybercrime?

4: Partner engagement

Possible issues to consider include:

- Data sharing risks
- The risk of partnering with an organisation involved in SOC activities.

Case study: Data sharing risks

Charity D supports bullied and isolated young people. The charity is approached by someone who offers use of their organisation's premises as a potential venue for group activities for free. In exchange, the person wants the names and contact information of all the young people supported, so they can share the 'house rules' and provide directions and so on. The charity obtains the permission of the young people to share this information and sends it to the person concerned. Subsequently, the person who made the offer withdraws it, citing insurance concerns for the premises. Weeks later, one of the young girls supported by the charity reports to the police that she has developed a relationship with an older man who initially approached her via email, befriended her and empathised with her problems, but has become abusive and is trying to get her involved in drugs and prostitution. It becomes clear that a gang involved in SOC exploited the charity for access to contact information for vulnerable girls.

Checklist 4: Partner engagement

Does your organisation:

- [ ] a) Disseminate your understanding of the risks of SOC to other stakeholders?
- [ ] b) Make use of technology (e.g. your website, social media) to disseminate information about the risks posed by SOC?
- [ ] c) Have arrangements in place for both internal and external data sharing?
- [ ] d) Have arrangements in police to share information/ intelligence with Police Scotland or any relevant regulatory body?
- [ ] e) Have regular meetings with Police Scotland or other partners to discuss the sharing of information/ intelligence?

5: Fundraising

Possible issues to consider when fundraising include:

- Receiving funds from an individual or organisation linked to SOC
- Receiving in-kind support from an individual or organisation linked to SOC.

Case study: Fundraising

Charity D is a small organisation with 2 paid members of staff and ten volunteers, who take young people on day trips to the countryside. The charity gratefully accepts a surprise substantial financial contribution from a new donor. The new potential patron is a local businessman involved in a range of different ventures including international transportation and haulage, and expresses an interest in becoming a trustee, as well as promoting the charity and his connection to it. The charity is unaware that this man is deeply involved in SOC, including people-trafficking of vulnerable women from around the world for forced work in the sex industry. He is seeking to legitimise himself and his businesses to provide further cover for his illicit activities. He has been the subject of many public controversies and is known to the police across the country. When the charity launches a publicity drive which highlights their donation and new connection, a tabloid newspaper runs an exposé which is highly damaging to the reputation of the charity.

Checklist 5: Fundraising

Does your organisation:

☐ a) Have measures in place to reduce the risk of receiving funds from an individual or organisation linked to SOC?

☐ b) Carry out background checks on potential donors and supporters to establish their trustworthiness? (i.e. Open Source, Companies House, Experian)

6: Commissioning, procurement and funding

Possible risks to consider include:

- Unknowingly providing funding to a third party with links to SOC
- Unknowingly purchasing goods or services from organisations with links to SOC.

Case study: Purchasing services

Charity G provides a befriending service and supports people with disabilities to take part in various community events and social activities. Due to the needs of the people using the services, transport by taxi is often required. When shopping around for the most cost-effective way of meeting this need, the charity are approached by a local taxi firm who offer a very cheap rate for contract taxis, which the charity eagerly accepts. Unbeknown to the charity, this taxi firm is deeply involved in organised crime. The drivers are often unlicensed, members of a criminal gang involved in drug dealing, violence, and exploitation and coercion of vulnerable people into criminal activity. They have been publically accused of involvement in these activities, and are known to the police and many in the local community. The gang uses the taxi firm to launder money, courier drugs, and potentially to identify vulnerable people or properties.

Checklist 6: Commissioning, procurement and funding

Does your organisation:

- [ ] a) Have measures in place to reduce the risk of providing funding (cash or 'in kind) to or buying goods/ services from an organisation with links to SOC?
- [ ] b) Undertake supplier checks for links to SOC as part of the procurement process?
- [ ] c) Make your staff with purchasing responsibilities aware of the risks of transacting with an organisation linked to SOC?
- [ ] d) Have a clear process for staff to raise any potential concerns about organisations with which your organisation contracts?

7: Physical assets, including cash and data

If your organisation has any assets, there is a potential risk to consider. For example, if properties owned by your organisation are being used or sub-let:

- to an individual or organisation with links to SOC
- for SOC activities (e.g. cannabis cultivation, prostitution, people trafficking, counterfeiting).

The data your organisation holds is also an asset which can potentially be targeted by groups involved in SOC.

Case study: Properties being used to support SOC

Charity C are a housing association with a number of properties specifically for the use of people with additional support needs including learning disability. A group involved in SOC has identified one of the charity's tenants, a vulnerable young man with limited social supports, as a target for exploitation. Over time, the gang befriends him, wins his trust, and begins to use his residence as a base for the production and distribution of drugs. The tenant develops drug addiction problems, and is also the victim of physical harm and extortion. Due to complaints from neighbours about anti-social behaviour, the police visit the address and discover the drug production. The tenant is arrested, detained and charged a range of drug offences, ultimately resulting in conviction and imprisonment. The property cannot be used until eviction processes have been completed, and the substantial damage to the property is repaired. During their time in prison, the tenant has accumulated rent arrears and must present as homeless upon release.

Case study: Data

Charity X provide housing advice support services to people with a range of issues related to poverty and addiction. They maintain a database of personal information about the people using the support services, including identity, personal needs and financial details. The charity do not maintain an ongoing IT support contract, preferring to use the inexpensive services of a friend of a former employee on a semi-regular basis. On one occasion, an unknown person arrives at the office to do some work, saying that the usual person was unable to attend so sent him instead. After he leaves, the charity discovers it has been locked out of all its systems, and receives a message from the hacker threatening keep them locked out and to release all the charity's data unless they pay a substantial sum. A number of the charity's service users receive blackmail and extortion messages.

Checklist 7: Physical assets

If your organisation has property, do you:

- [ ] a) Have a way of checking that none of your properties are being used to further SOC (e.g. cannabis cultivation, prostitution, sub-letting, people trafficking)?

- [ ] b) Have processes in place to ensure that any maintenance and repair to your property is not being performed by organisations with links to SOC?

- [ ] c) Make your tenants aware of the risk posed by SOC in the community? How would tenants report any concerns to you?

Annex A: Sources of Further Information and Support

Should you have concerns or suspicion that somebody is involved in or directing serious organised crime you should report it to **Crimestoppers** on **0800 555 111** or to your local police office.

In an emergency, always call 999.

For information about….

Online safety for young people: **www.**thinkuknow.co.uk

The dangers of smoking, alcohol and drugs as well as online safety and advice on how to deal with negative peer pressure: **young.scot/choices-for-life**

Issues relating to modern slavery: **www.modernslavery.co.uk**

Fraud and financially motivated internet crime: **www.actionfraud.police.uk**

Financial crimes: **www.hmrc.gov.uk**

Business security services and advice, visit: **www.sbrc.org.uk**

Online threats and how to reduce your exposure to these: **https://www.ecrimescotland.org.uk**

How to protect yourself, your computers, mobile devices and organisation against fraud, identity theft, viruses and other problems encountered online: **www.getsafeonline.org**

The collaborative Building Safer Communities programme, which seeks to help national and local partners and communities work together to make Scotland safer and stronger: **www.buildingsafercommunities.co.uk**

Information for Victims, witnesses or people charged with an offence, visit: **www.crownoffice.gov.uk**

About CJVSF

The Criminal Justice Voluntary Sector Forum (CJVSF)**:**

- Supports voluntary sector providers to continuously improve their own criminal justice services through collaboration and sharing of good practice
- Assists voluntary sector providers to understand, navigate and influence the complex and changing environment in which they operate
- Promotes broader awareness of the activities, value and impact of voluntary sector services within criminal justice.

The CJVSF is hosted by CCPS (the Coalition of Care and Support Providers in Scotland). Further details about the Forum can be found at: www.ccpscotland.org/cjvsf