ico.
Information Commissioner's Office

Findings from ICO advisory visits and contact with Victims' Services Alliance Organisations

Date issued: 22 January 2015

Executive summary

The Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the Data Protection Act 1998 (the DPA) and for promoting good practice in information handling. The Act consists of eight principles of good information handling that all organisations processing personal data have to comply with.

During 2014, the ICO Good Practice department undertook three voluntary data protection advisory visits and two teleconferences with charitable organisations who are members of the Victims' Services Alliance (VSA). In addition, the ICO also sent a snap survey to all 69 VSA member organisations. The scope of these visits and meetings focussed on the technical and organisational measures in place to address the following key issues:

- Data protection roles and responsibilities of staff and managers
- Physical security
- Access controls – network and user
- Training and awareness
- Data security incident reporting
- Home/mobile working, including the use of portable media devices
- Collection of data/fair processing notices
- Maintenance, indexing and tracking of records (including data quality)
- Retention schedules and disposal of data
- Data sharing and the transmission of personal and sensitive personal data via email
- Awareness of Subject Access Requests (SARs)
- How SARs are identified and processed

The objective was to understand how these organisations are processing personal data across the consortium. This report is aimed at all member organisations within the VSA and other charitable and non-charitable organisations that provide similar services.

The outcomes of our study varied across the member organisations that took part; however the following key themes were identified:

- Staff generally have a good awareness of the requirement to keep all personal data safe and appear keen to comply with the DPA.
- Physical building security is generally adequate with access and movement within premises being managed through controls, such as manned receptions, visitor procedures and appropriate siting or obscured views of hardware processing personal data.
- Portable and mobile devices, including magnetic media, used to transport and store personal data are not being adequately

protected. All USB ports and other drives which can be used for removable media must be locked down.
- Examples were found where information was being retained for longer than is necessary. All VSA organisations should review the types of records holding personal data and identify how long they need to be retained after the relationship with the client, employee, counsellor or therapist ends. If the information is no longer required, then it should be securely destroyed.

Contents

This report covers the following:

- Our approach to working with VSA organisations to produce this outcomes report.
- A background to the VSA – who they are and the services they provide.
- The types of personal information processed by organisations within the VSA and the issues to consider in order to comply with the DPA.
- Areas of good practice that were seen or demonstrated during our study.
- Areas where improvements could be made, or where common issues or themes were found that other organisations can learn from.

Approach

The ICO's advisory visits are one day informal visits to look at how an organisation handles personal information. Teleconferences can also be held as an alternative to an on-site visit and follow the same scope areas and format as a visit.

Five VSA organisations contacted the ICO to request practical advice and guidance through either a visit or a teleconference meeting. We also ran a voluntary survey for member organisations from 14 to 31 October 2014 and we received 27 anonymous responses.

This report explains the areas where VSA organisations appear to be performing well, as well as highlighting the common problems and areas for improvement that other organisations can learn from. The report includes further guidance and advice to help organisations improve their data protection practices.

Background - Victims' Services Alliance

The VSA launched in December 2011 and initially consisted of organisations who work with individuals and families bereaved by murder, manslaughter and road deaths. They now offer membership to all organisations working with victims of crime beyond the scope of homicide.

The VSA is a national network of 69 third sector agencies who work together to improve services to victims of crime, their families and others who may have been affected by the crime. This is achieved through collaboration; influencing and engaging with government and key decision makers; and the sharing of ideas, resources and good practice across the member organisations.

The Alliance meets four times a year, allowing members to share updates, network, discuss issues of concern and meet with key people within the criminal justice system.

The Code of Practice for Victims of Crime (October 2013) requires the police and other criminal justice organisations to provide services to victims including bereaved close relatives and states that the information shared between organisations must be done so effectively and in accordance with the DPA. Other organisations, including voluntary sector organisations, may provide services for victims but they are not covered by this code.

Police forces and Police and Crime Commissioners have responsibility for commissioning victim services in their areas, different models will operate in different areas but an increasing number of third party providers will be used. This report will assist in ensuring all VSA organisations are aware of their responsibilities under the DPA.

Typical processing of personal data by victims' services alliance

Organisations operating within the VSA process a significant amount of highly sensitive personal data and share this with other bodies, including the police. This information is in paper and electronic form and will relate to criminal and civil investigations involving victims, their families, witnesses and, in some cases, suspected perpetrators. The details will include, names, addresses, medical reports, information about the services required and delivered and staff employment records.

Information is held on personal and charity computers within databases and email accounts. A significant amount of manual data is held within filing cabinets on agency premises, employee home addresses or is archived and managed by a third party organisation. It is usually transferred electronically by email, but in some instances the information is sent by post.

Many VSA organisations rely on volunteers and temporary staff to process personal data and deliver the various services they provide. The survey confirmed 69% of organisations had more than 20 volunteers working for them. This provides challenges due to the potential for a high turnover of staff and the need for all of these volunteers and temporary staff to be made aware of and comply with their responsibilities under the DPA.

Areas of good practice

The VSA organisations we visited, or had contact with, demonstrated the following examples of good practice:

- ✓ Staff generally have a good awareness of the requirement to keep all personal data safe and appear keen to comply with the DPA.
- ✓ Staff are aware of the requirement to only collect personal data that is adequate and relevant for the purpose.
- ✓ The majority of staff and volunteers are vetted by the Disclosure and Barring Service (DBS). The survey confirmed 85% of all staff are required to undertake vetting before they are appointed.
- ✓ The Criminal Justice Secure Mail (CJSM) email system is used for referrals to and from other agencies. The survey confirmed 44% use the CJSM to transfer personal data to other organisations.
- ✓ Access to the networks VSA organisations are using is immediately disabled as soon as a member of staff leaves the organisation.
- ✓ Personal data is anonymised before statistics are shared with funders or used for management information.
- ✓ During written communication unique reference numbers, initials or first names are used instead of the person's full name.
- ✓ Building security is generally good, with access and movement within the premises used by VSA organisations controlled. The

survey confirmed 80% of organisations have either a manned reception or clear visitor procedures in place, or both. The windows in the offices visited had frosted glass and blinds that stop anyone who walks past the building viewing any personal information available on employees' desks or computer screens.

✓ Systems will lock down following a restricted number of failed log on attempts.

✓ A cross cut shredder is used for day-to-day destruction of unwanted information.

The good practice examples identified within this report were not always consistent across all organisations the ICO visited or spoke to, however it was evidenced in at least one VSA organisation that participated in the study.

Main themes and areas for improvement

As a result of the ICO's study, the following themes and areas for improvement were identified and should be considered as a priority for all VSA organisations:

! **DATA CONTROLLER AND PROCESSOR**

Finding: Some counsellors and therapists are sub-contracted by organisations to provide specialist counselling to clients. Agreements they sign do not always refer to data protection, information security or any records management procedures. It is unclear, in terms of the DPA, who is the data controller or data processor and what would happen to the personal data they are holding should the relationship with the organisation break down, or the agreement be terminated.

Recommendations: Organisations should refer to the ICO's data controllers and data processors guidance which explains the difference between both categories and the implications for the organisations concerned. Once the relationship has been determined, this should be formally documented along with the relevant roles and responsibilities. Create a counsellor's agreement which covers, as a minimum, the security provisions that are expected for any documents containing personal data about a client, and the response times that are expected to be met for any requests for information from management.

! HOME AND REMOTE WORKING

Findings: The survey shows that 41% of staff working for VSA organisations work from home. However, there did not appear to be any agreed process setting out responsibilities for home workers in relation to how paper documents or mobile devices should be used off-site or secured while in transit. There was a lack of process or guidance for tracking the whereabouts of records taken away from the office.

Recommendations: Organisations should have a formal home and remote working policy in place to ensure personal information continues to be handled correctly outside of the office. The policy should make sure that staff are told to keep personal information in a locked case when not in use and should not be left unattended. Organisations should keep a record of personal information removed from the office and make sure any information is securely destroyed once it's no longer needed.

! RETENTION SCHEDULE

Findings: Most of the VSA organisations covered in this report do not have a retention schedule in place to ensure that all personal data is only held for an appropriate length of time in a controlled environment. The survey revealed some manual documents are archived in the loft of employee private premises. The survey also showed that 11% of manual records and 15% of electronic records are held indefinitely. This would be considered a breach of the 5th principle of the DPA and will mean that the information is likely to become increasingly inaccurate over time.

Recommendations: Organisations should review the types of records containing personal data and identify how long they need to be retained after the relationship with the client, employee, counsellor or therapist ends. Any records that are no longer required should be securely destroyed.

The length of time that an organisation should keep personal data depends on the purpose for which it was obtained and the nature of the information. If it continues to be necessary to hold the data then it should be retained for as long as that reason applies. Consideration should be given to:

- Legal and regulatory requirements.
- Standard industry practice.
- Past experience – historically, how many files are needed or requested?

Further information to help create an appropriate retention schedule can be found in the ICO's guidance on Principle 5 of the DPA.

! DATA SHARING

Findings: The sharing of sensitive personal data is conducted on a regular basis and can be carried out in response to ad hoc requests with other agencies if there is a statutory requirement, legal basis or safeguarding reason for doing so. The survey results indicate that sharing takes place with various organisations such as other charities, the police, the NHS and the local council. However, during our visits several staff reported they were not aware of any formal data sharing agreements being in place.

Requests for personal data are generally reviewed and authorised by a senior member of staff. However, there was limited evidence of exemptions or redactions being applied prior to the disclosure or any record of the rationale and decision making process.

Recommendation: Organisations should follow the guidance in the ICO's Data Sharing Checklist and Data Sharing Code of Practice and ensure that information shared on a regular basis is covered by a data sharing agreement signed by all relevant parties and regularly reviewed.

! SECTION 29 EXEMPTIONS

Finding: Section 29 of the DPA includes an exemption that allows for VSA organisations to share personal information for the prevention and detection of crime. However, there are limits on what can be released. Our study did not provide us with assurances that all VSA organisations fully understood and were confident in determining whether a Section 29 exemption would apply when supplying information to relevant third parties.

Recommendation: Organisations should consider whether this exemption applies on a case-by-case basis before releasing the information. The exemption only allows organisations to release personal information for the stated purposes and only if not releasing it would be likely to prejudice (that is, significantly harm) any attempt by the police to prevent crime or catch a suspect. Further guidance on the exemption under the DPA covering the prevention of crime can be found on the ICO website.

! WINDOWS XP

Finding: Around a third of the VSA organisations surveyed are still running the Windows XP operating system. This system is no longer supported by Microsoft and will become increasingly insecure over time.

Recommendation: Organisations should only be using supported operating systems that the manufacturer provides regular security updates for. Those organisations still using Microsoft XP should migrate to a supported platform as a priority.

! ENCRYPTION

Finding: The laptops used by staff to store and transmit personal information do not have encryption. This would not be considered as providing adequate security in circumstances where the loss or corruption of the information could cause substantial damage or distress to the individuals affected.

Recommendation: Organisations using portable and mobile devices to process this type of personal information must use approved encryption software. This will make sure that the information remains protected in the event that the device is lost or stolen.

! THIRD PARTY IT PROVIDER

Findings: Some organisations outsource their IT requirements to a third party contractor. The survey found that 77% of organisations use third party service providers for IT, HR, archiving and confidential waste. However, in many cases there were no formal contracts in place to ensure that the personal information handled by these third parties continued to be looked after in compliance with the DPA.

Recommendations: Organisations must have a contract in place with third party providers handling personal information on their behalf. Organisations should also be satisfied that the third party will continue to maintain the same level of security as the organisation would. Regular checks should also be carried out to ensure compliance with the provider's security procedures. Further information can be found in the ICO's guidance on keeping personal data secure.

! DISPOSAL OF HARD DRIVES

Finding: A number of 'end of life' computers are being insecurely stored either on site or off site at home addresses.

Recommendation: Organisations should remove and securely destroy the hard drives of any 'end of life' computers that are no longer required. The remaining computer components and hardware can then be recycled. Read the ICO's deleting personal data guidance for further information on the options available for secure deletion.

Other areas for improvement

! BRING YOUR OWN DEVICE (BYOD)

Finding: Some employees use personal devices, such as their personal laptop, smartphone or USB memory stick, in the workplace for business purposes. Allowing devices that the organisation does not have sufficient control over to connect to the corporate IT systems can introduce a range of security vulnerabilities and other data protection concerns if not managed correctly.

Recommendation: Organisations should follow the advice in the ICO's Bring Your Own Device (BYOD) guidance. The guidance explains the measures all organisations should have in place when allowing staff to use personal electronic devices for work purposes.

! TRAINING

Findings: During the ICO's advisory visits and calls it was found that there is little or no data protection or information security training provided to new members of staff. The survey suggested that 80% of those participating received training in the last 12 months. However, the ICO is unable to view the standard of this training, or the frequency with which it was delivered.

Recommendations: Organisations should make sure all employees at all levels, including volunteers, contractors, counsellors and therapists, are made aware of their roles and responsibilities to make sure people's information is looked after in compliance with the DPA. Appropriate data protection and information security training should be introduced as a priority for all existing staff. New employees should receive data protection training as part of their induction course.

Organisations should:

- keep a record of staff who've completed their data protection training;
- carry out regular assessments and refresher training to make sure employees' knowledge remains up-to-date; and

- get staff to read the organisation's data protection policy or procedure and sign to confirm that it has been fully understood.

! CLEAR DESK AND SCREEN

Findings: Not all of the VSA organisations contacted operate a clear desk and screen policy with paper records often left on desks or printers. Some files were left in insecure cabinets or open shelving. The use of "Ctrl-alt-delete" to lock work station screens was inconsistent. The survey also revealed that while 67% of employees did adhere to the clear desk and screen policy, only half confirmed that spot checks are carried out to monitor compliance.

Recommendations: Organisations should develop a formal clear desk and screen policy and communicate it to all staff and any relevant volunteers, including home workers. The policy should include a requirement to maintain clear desks and secure personal data away in lockable filing cabinets and drawers when it's not in use and at the end of the day.

Printers and fax machines should be checked to make sure information is not left unattended during the day or overnight. Staff should also be told to lock their workstations using "ctrl-alt-delete" when not in use and monitor compliance.

! NETWORK OR SYSTEMS BACK-UP

Finding: Some organisations are able to control their own network access for staff and conduct regular backups of their system. However, the backups were not always stored securely. According to the survey 16% of organisations do not back up their data and 24% use a cloud provider.

Recommendation: Organisations should make appropriate arrangements to ensure that system back-ups are kept secure. If personal data is accidentally lost, altered or destroyed organisations should have a process in place to ensure that it can be recovered to prevent any damage or distress to the individuals concerned (See also recommendation for third party IT provider).

! INCIDENT AND BREACH REPORTING

Findings: Not all security breach incidents or near misses are recorded or reported, and staff were often unaware of any policy or procedure to follow if there is a security incident or breach.

Recommendations: Organisations should have a formal process in place for reporting, logging and investigating every information security incident. Further advice can be found in the ICO's guidance on data security breach management. Breaches or near misses should be communicated to all staff so they are aware of any 'lessons learned'.

! INTERNET USE, WEB FILTERING & ANTI-VIRUS

Findings: Some organisations only have the standard antivirus and malware protection provided by Microsoft's operating system. This may not be adequate to protect sensitive personal information.

Most VSA organisations also didn't appear to have any blocks on unsuitable websites, such as social media or webmail clients. This meant that staff could, in theory, upload organisational and client information to the internet or unknowingly download malware that might compromise the network.

Recommendations: Organisations should make sure that appropriate anti-virus and malware software is installed on their computers. They should also ensure that web filtering is carried out to stop their staff accessing inappropriate or high risk sites, such as social media and webmail clients. Further guidance can be found on the GetSafeOnline website.

! SERVERS

Finding: Some organisations onsite servers were found to be located in unlocked offices. The server is critical to the running of the organisation and if tampered with, or damaged in any way, could cause serious disruption or the loss of data.

Recommendation: Organisations should ensure servers are located in separate locked rooms with access to the room strictly controlled.

! FAIR PROCESSING

Finding: There is currently no fair processing notice on some organisations' websites or any further information to explain to people how their information may be used or disclosed. This includes disclosure for safeguarding purposes.

Recommendation: Organisations should create a standard fair processing notice that must be shared with new clients, either verbally or in writing. The notice should be made available on the organisation's website. The notice should outline the type of data that may be shared and the circumstances when this would occur. Further guidance on

how to draft an appropriate privacy notice can be found in the ICO's Privacy Notices Code of Practice.

! PASSWORDS

Findings: Some staff didn't have individual log ons or unique passwords to access their organisation's systems. Examples were also found where passwords were routinely shared or written down. VSA organisations did not provide any guidance to staff advising them on the length or complexity of passwords, the frequency with which passwords must be changed or the number of failed attempts that were allowed before the system would lock them out.

Recommendations: Organisations should endeavour to ensure that every user has their own username and password. Where this is not possible, organisations should ensure there are appropriate controls in place to maintain an effective and robust audit trail and prevent fraudulent activity. There should be standard minimum security requirements established for the setting of passwords across all systems, including desktop computers, laptops and mobile phones.

These requirements should require staff to:

- change their temporary password after they've logged on for the first time;
- use a strong password that is at least eight characters long and includes a mixture of upper and lower case letters, numbers and characters; and
- not to share individual passwords with other members of staff.

Organisations should also:

- prompt users to change their password on a regular basis; and
- restrict the number of failed login attempts before the staff member is locked out and requires an administrator to let them back into the system.

These rules should be formally recorded in the security policy.

! PRINTING AND FAXING

Findings: Some premises have either shared all-in-one machines that are capable of printing and faxing or separate printer and fax machines. In both circumstances the VSA organisations contacted had no measures in place to ensure printing or faxing takes place in a secure manner.

Survey responses indicated that 78% of organisations that completed the questionnaire do not have secure printing. This creates a risk that sensitive personal data could be left at the printer and be accessed inappropriately, or inadvertently incorporated into another person's printing and even sent to the wrong client. There were also no procedures or guidelines on using fax machines securely and ensuring faxes reached the correct recipient.

Recommendations: Organisations should introduce secure printing technology, including the appropriate use of PIN codes or security cards which staff are required to use. If this is not possible then VSA organisations should create a secure printing procedure that explains that staff should collect their prints as soon as they send documents to the printer. Communicate this requirement and reinforce with posters or email reminders. Provide a set of rules for staff to follow should they need to use the fax machine to transfer information to another organisation.

! ENDPOINT CONTROLS

Finding: The survey found that one in three responders could use their own USB or memory stick as USB ports were not locked down. This raises a significant risk of unauthorised uploading or downloading of personal information, as well as the potential for the introduction of malware without the organisation's knowledge.

Recommendation: Organisations should ensure that all USB ports and other drives that can be used for removable media should be locked down. Staff with a legitimate business reason could be granted the ability to use certain ports when required. However, this should only be done using encrypted USB sticks provided by the organisation. VSA organisations should also keep a log of the authorised portable media devices given to staff.

! POLICIES AND PROCEDURES

Finding: Based on the advisory visits and teleconferences conducted, several organisations do not have specific data protection or information security policies or procedures in place. The survey results contradicted this, with 96% of the VSA organisations who responded reporting that they have appropriate policies and procedures in place. The ICO was unable to use the survey to establish whether staff knew where to find the related policies, or if they are being reviewed on a regular basis and remain fit for purpose.

Recommendation: It is essential that organisations ensure appropriate data protection and information security policies and procedures are in place. These documents should be signed off at a board or trustee level and communicated to staff, including volunteers and home workers. The policy and procedures document should be stored on the organisation's intranet, or on a shared drive for easy access. Policies should be reviewed on a periodic basis and updated when necessary.

! RETENTION - ASSET REGISTER

Finding: All of the VSA organisations covered by this report didn't have asset registers in place to explain what devices were being used to process personal data. Without a register there is a risk of the organisation not being aware if a device goes missing.

Recommendation: Organisations should produce asset registers that list all of the devices they own, who is using them and where they are located.

! PRIVACY IMPACT ASSESSMENT

Finding: There was no evidence that any PIAs are conducted when procuring new - or making significant changes to - ICT systems and data handling processes to identify and address information risks in the early stages of a project.

Recommendation: Organisations should read the ICO's recently updated Privacy Impact Assessments - Code of Practice. The code explains the privacy issues that organisations should consider when planning projects that use personal information, including the need to consult with stakeholders, identify privacy risks and address these risks in the final project plan.

! SUBJECT ACCESS REQUESTS

Finding: The ICO identified that VSA organisations had received subject access requests from data subjects, or requests for personal information from third parties. However, evidence suggested that there were no formal procedures in place for recognising, logging and responding to such requests when they are received.

Recommendation: Organisations should create an 'Access to Information Policy' so that staff are able to recognise and respond to requests from data subjects and third parties appropriately. For further information please see the ICO's Subject Access Request Code of

Practice and the Subject Access Request Checklist and Data Sharing Code of Practice available on the ICO website.

! EMAIL

Finding: Unsecure email accounts are being used to send and receive emails containing personal data in the office and by home workers. The survey found that 41% of responders are not required to use file passwords or encryption software when sending external emails, and 22% didn't know whether emails they sent were encrypted or not. If leaked, lost or stolen, information relating to victims, witnesses and alleged perpetrators (suspects) has the potential to cause significant damage and distress to those concerned and their families. Such incidents could also seriously damage the organisation's reputation.

Recommendations: Organisations should contact their IT provider to request that a secure email client is provided. Staff should also be able to use the encryption tools offered on standard software packages so they can encrypt documents containing sensitive personal data before they are sent via email.

Alternatively, organisations should request access to the Criminal Justice Secure email (CJSM) which is utilised by several other charities and criminal justice practitioners that have insecure email or fax and work within the criminal justice system. Once implemented, a formal procedure should be produced that explains to all staff, including home workers, how personal information should be handled when using email.

! INFORMATION RECORDING STANDARDS

Finding: Some organisations didn't have documented standards or guidelines for staff to ensure the information they record is accurate, adequate, relevant and not excessive. There are particular risks in recording the details of third parties in unsearchable fields.

Recommendation: Organisations should create information recording standards for staff, train them in their use and implement appropriate quality checks. This will ensure compliance with the 3rd, 4th and 5th principles of the DPA. Organisations should also include instructions to minimise the amount of third party data embedded within free text fields, as searching for this data may prove problematic.

! MARKETING

Finding: Charity organisations regularly send emails to their list of contacts, members, clients or victims for 'marketing' purposes to raise

awareness of services; however recipients are not always offered the option to opt in or out of marketing email correspondence.

Recommendation: Charities should ensure they offer the option for recipients to opt in and out of email correspondence and to consider the possible implications and impact to those who might not want such communications. Any individual who requests not to be contacted for marketing purposes must be flagged as being 'suppressed' so that their personal information is not used for this purpose again in the future. The ICO's guidance on the Privacy and Electronic Communications Regulations (PECR) provides further guidance to help charities meet their legal requirements when carrying out marketing activities.

! **KEYS**

Recommendation: Organisations should consider using key cabinets or similar containers that require a PIN code to access. The code should be changed on a regular basis.

! **KEY CODE LOCKS**

Recommendation: Organisations should then ensure the codes for key cabinets are changed on a regular basis, including when a staff member leaves. This could be added to the information security policy.

Further guidance

The ICO has produced a range of guidance for organisations to use to better manage and secure their personal information:

- Guide to Data Protection
- A practical guide to IT security
- Checklist for handling personal information
- 'Think Privacy'
- The implementation guides for the National Archives Records Management Code of Practice (particularly Guide 8, relating to retention)
- Getting it right: small business checklist
- Taking a positive approach to information rights

The following guidance provided by other organisations may also prove useful.

- Council on cybersecurity - Interactive controls toolkit. The website provides drop down explanations and lists of vendors of resources designed to address key controls.
- Centre for Protection of National Infrastructure publish a range of security videos on its YouTube Channel
- Charity Finance Group - Protecting Data Protecting People - A Guide for Charities.
- Information Assurance and Cyber Security Engagement programme e-training course to protect against cybercrime.

Further assistance

The ICO also has a helpline with staff on hand to answer queries about data protection compliance on **0303 123 1113**.