Findings from ICO advisory visits to 32 charitable organisations

Background

The Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the Data Protection Act 1998 (the Act) and also has a remit 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.

In 2012/13 the ICO undertook **32 advisory visits** at various charitable organisations to gain a better understanding of the processing they undertake and the circumstances in which they operate.

Advisory visits are a one day informal visit to look at how an organisation handles personal information. ICO staff provide practical advice and guidance on site and a short report after the visit. The visits typically focus on information security and records management.

The charitable organisations visited during the period included regional charitable volunteer services, housing/tenant support services and children's/young adult support services. All but two of the organisations are registered charities within the UK.

The organisations visited varied considerably in terms of the numbers of staff and volunteers, the resources and facilities available to them and the sophistication of their systems and processes. However they also had many common themes because of the focus of the work they undertake.

This report highlights our experience of personal data handling by charitable organisations and is intended to help them see where they can make improvements in how they handle personal data.

Typical processing of personal data by charities

Charities process the information of their customers and employees / volunteers in paper and electronic form. This will include names, addresses, medical records or reports, services required and delivered, business funding records and staff employment records.

Of particular relevance is the high degree to which charities rely on volunteers to deliver services. This presents a particular set of challenges due to the potential for high turnover of staff and difficulties in ensuring that volunteers are aware of and comply with their responsibilities in relation to data protection.

Areas of good practice

✓ Over a third of charities visited granted **access to IT systems** and electronic data based on job role and a 'need to know' basis. This reduces the risk of inappropriate access to personal data by staff. In one particular case only a small number of vetted individuals were able to access a specific system.

✓ A similar proportion of charities provided **information to their customers**, in the form of fair processing notices, on the way their personal data is processed and which organisations it is shared with.

✓ Over a quarter were identified as having good **physical and building security** in place. This included the use of swipe card access, keypad or buzzer entry, lockable file units and unmarked locked archive and server rooms.

✓ Approximately a quarter of organisations visited had a formal **policy setting out data protection procedures** and the roles and responsibilities of staff in relation to personal data.

✓ A number of organisations were observed to have **confidential waste processes** in place which involved the use of secure bins and cross-cut shredders. This improves the security of personal data which is no longer required by the organisation.

✓ By being resourceful with the data they collected at registration, one organisation was able to produce a range of management information using their IT system without requiring further **details from individuals**; this reduced the risk of collecting excessive or duplicate personal data.

Areas for improvement

! Over a half of charities visited did not have **formal retention schedules** in place to ensure that the different categories of personal data held had been identified, and were only being kept for an

appropriate length of time. Such retention/disposal schedules help safeguard against the indefinite retention of personal data which would be a breach of the Act.

- More than a third of organisations also lacked **processes for the regular weeding of personal data held within manual records** to ensure they were not excessive, irrelevant or out of date. Implementing regular weeding processes reduces the risk of breaching the DPA, helps minimise the data held and therefore reduces the impact and/or likelihood of any personal data breach.

- Approximately half of charities had failed to **disable USB ports and DVD/CD drives** on computers to prevent unauthorised removal of personal data using portable media or the upload of malicious code to the network.

- A significant proportion of organisations visited did not have **minimum requirements for password complexity** or did not enforce regular password changes either automatically through IT systems or through a password policy.

- Over a third of charities visited did not have **annual refresher training** in relation to data protection for all staff who handle personal data, or more in depth training for specialised roles such as records managers, data protection officers and information security managers. Of particular importance is the need to ensure that volunteers processing personal data receive regular training or awareness sessions.

- A similar proportion did not have a **clear desk policy** in place or appropriate checks, for example regular after hours reviews were not carried out.

- A large proportion of charities did not have **adequate security in place** for manual records containing personal data. This may have been due to the lack of secure storage cabinets, failure to lock these cabinets or lack of secure storage for the keys to those cabinets.

- Approximately one in four organisations did not have **remote working procedures** in place. These should set out the technical requirements for secure homeworking, the responsibilities of staff in relation to personal data when working from home and the procedure for authorising remote working.

- A similar number of charities did not have **secure fax or printing procedures**, such as pin-coded printing or swipe cards, in place.

! A significant proportion of charities lacked robust **procedures for controlling access to personal data for new starters**, those moving to different positions within the organisation and those leaving it. This is a particular risk area when there is no defined period of employment or staff are not employed directly by the organisation; for example where temporary staff or volunteers are used. Proper procedures in this area help reduce the risk of unauthorised or inappropriate access to personal data, and prevent the accumulation of access rights that are not relevant to an employee's current role.

More information

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

- Charity sector guidance
- Data protection guidance

Other useful guidance:

- A practical guide to IT security (pdf)
- Employment code of practice – quick guide (pdf)
- CCTV code of practice
- Privacy notices
- Checklist for handling personal information (pdf)

Find out more about our advisory visits and read summaries of advisory visits we've carried out.

Further assistance

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