Findings from ICO advisory visits to independent fostering and adoption agencies

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 2013 the ICO's Good Practice department delivered 10 data protection advisory visits for independent fostering and voluntary adoption agencies. The sector was chosen on the basis that organisations operating within it process a significant amount of sensitive personal data and share this with other organisations, notably local authorities.

Advisory visits are one day informal visits 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 with recommendations for improvement. The visits typically focus on information security, records management and requests for personal data.

The 10 visits formed the basis of a project designed to identify common problems, issues and themes in relation to the processing of personal data in the fostering and adoption sector, and to provide it with relevant data protection advice and guidance.

Originally twenty organisations were approached to see if they were interested in receiving an advisory visit. Some were selected from a list published on the Consortium of Voluntary Adoption Agencies' (CVAA) website and others from a list published on the British Association for Adoption and Fostering's (BAAF) 'Be my parent' website. In addition, other agencies were invited following previous contact with the ICO either via a written request for specific advice or because a complaint had been submitted about them.

Fostering agencies

Under the Children Act 1989, local authorities are obliged to provide suitable accommodation for children in their care. One of the ways in which they do this is via foster carers registered with Independent Fostering Agencies (IFA's). Most IFAs have charitable status or are profit making, charging fees to local authorities where they have used the IFA's foster carers. They are bound by legislation, including The Fostering Services (England) Regulations 2011 and the Fostering Services National Minimum Standards, as well as statutory guidance, in particular the Children Act 1989 Guidance and Regulations Volume 4: Fostering Services. In addition, they are regulated and inspected by Ofsted.

Adoption agencies

Adoption services are usually run through local authorities; however, there are some voluntary adoption agencies and a few 'hybrid' agencies that recruit both foster carers and potential adoptive parents. Prospective adoptive parents can choose to register with either type of organisation. Local authorities are responsible for finding adoptive parents for children that require them, although they will usually seek parents from a different area than the one in which the child is in care. Local authorities may therefore select adoptive parents registered with VAAs. Voluntary agencies usually have charitable status and are funded by donations, fund raising and fees charged to local authorities. They are bound by legislation including the Adoption and Children Act 2002, the Adoption Agencies Regulations 2005 as well as Statutory Guidance on Adoption. They too are regulated and inspected by Ofsted.

Typical processing of personal data by independent fostering and adoption agencies

Fostering and adoption agencies process highly sensitive information in both paper and electronic form relating to foster carers, adoptive parents and looked after children and their families.

Potential foster carers/adoptive parents provide their personal information to agencies in order to be assessed for their suitability for adoption/fostering. Much of this information must be forwarded to an independent panel that participates in the approvals process. It includes information such as medical history, marital status, relationship information, employment, criminal convictions, religious beliefs etc. Within fostering agencies this information is collected within an assessment report.

Local authorities send profiles of looked after children requiring foster placements or children awaiting adoption to the agencies so that they can identify suitable matches. These profiles include medical history, birth parent information, previous placement information, ethnicity, educational achievement, behavioural issues, etc.

Agencies then send detailed information about suitable carers/prospective parents to the local authority in order to facilitate a match. This presents a particular set of challenges due to the requirement for very sensitive information to be shared quickly and easily. In the case of fostering agencies this requirement is often intensified by their desire to quickly secure commercial contracts with local authorities.

Information is held on computers within databases. A significant amount of manual data is held within filing cabinets on agency premises or is archived and managed by a third party organisation. It is usually transferred by email but sometimes by post.

Main themes and observations

! Highly sensitive personal information (including medical history, marital status, sexuality, relationship information, employment, criminal convictions and religious beliefs) concerning foster carers and looked after children is routinely emailed between agencies and local authorities for the purpose of arranging foster care placements, without encryption safeguards in place. The lack of such safeguards increases the risk that the information could be inappropriately accessed and there would appear to be a number of factors contributing to this practice:

- It was reported that local authorities are often reluctant to accept encrypted information via email as their IT security systems block the messages and it can be time consuming and difficult to liaise with their IT team to unblock them.
- In addition, it was suggested that local authorities may not wish to deal with a multitude of encryption programs being used by different agencies.
- Foster agencies in particular often send this information without encryption because they feel that if they do not provide a quick means for local authorities to access their foster carer's information, a local authority will simply use another fostering service.

! The majority of agencies visited did not encrypt mobile devices used to process, store or transport personal data. This included items such as laptops and USB sticks. If lost or stolen, any such devices containing sensitive personal data could be easily accessed. Where such losses occur and encryption has not been used to protect the data, the ICO is more likely to pursue regulatory action.

! Fostering agencies often require carers to provide them with updates about looked after children but they do not provide secure methods such as VPNs by which to do this. Sensitive personal information is therefore processed on home computers and stored in the 'cloud' in ISP or webmail accounts (Hotmail, Gmail etc.). As data controllers, agencies are responsible for this information and they must ensure it is stored/transmitted securely and disposed of when no longer required.

Agencies should also provide clear guidance on what carers should include in these updates to ensure that the personal data processed is relevant and not excessive.

! Some agencies allow their staff to carry out work involving sensitive personal data on their home computers instead of providing appropriate remote access to their network, an encrypted memory stick or a work issued encrypted laptop on which to save their work. This information can then be saved or printed on home computer systems, raising numerous risks in relation to security, access, retention and deletion of looked after children and foster carers' sensitive personal information.

! Adequate data protection/information security training is not provided by agencies to their staff. Specific data protection/information security training should be provided at induction and refreshed periodically thereafter so that staff are aware of the required security procedures around personal information and their obligations under the DPA.

Other areas for improvement

! In most agencies visited staff passwords allowing access to network and information systems are not changed on a regular basis and some agencies did not enforce the use of complex passwords. When password controls are not robust, agencies are at risk of internal unauthorised access to information or facilitating external attacks of IT systems e.g. their WiFi network.

! Secure printing procedures are not widely adopted to ensure that confidential information is not left on printers or gathered into other printed material.

! Endpoint controls (restrictions on the use of removable media) are often not in place, which may result in sensitive personal data being extracted from IT systems without the organisation's knowledge or the IT systems being deliberately or inadvertently infected with viruses or malware.

! The majority of agencies did not have policies covering building security, information security or data protection. This leads to a lack of clear direction and strategy in these areas, and the adoption of inappropriate or inconsistent procedures by staff.

! Few agencies had information security breach procedures in place to monitor, record and investigate any information related security

incident. This results in an organisational lack of awareness of breaches, systems/process weaknesses and means that appropriate remedial action is not instigated.

! The nature of the sector and the significant volume of sensitive personal data being created and exchanged within it leads to a real risk that some of the information processed/held is either excessive, retained for longer than necessary, or both. Few agencies had retention and disposal policies or schedules setting out what records should be retained, for how long and how they should be securely destroyed when no longer required. Agencies should consult relevant legislation and guidance (such as that referenced earlier) in order to determine retention periods. If no legal requirement exists to retain the personal data they hold, agencies should ensure they set and implement retention periods that reflect only specific business needs.

Areas of good practice

✓ Most agencies visited had adequate IT access controls based on individuals' job roles to reduce opportunities for unauthorised access, modification or misuse of information, or services. Access to systems is amended when staff change roles and is revoked when they leave.

✓ The best organisations set out home working rules and requirements within a policy and carried out periodic inspections to ensure compliance. These policies include the requirement to have a suitable place to work and somewhere secure to store manual records, removable media and laptops.

✓ Foster carers are sometimes required to have a secure place to store foster placement information, usually a lockable cabinet.

✓ Quality checks to ensure that records were fit for purpose, accurate and up to date were carried out by two agencies.

✓ One agency with several sub branches plans to develop a system of information asset owners reporting to head office on the security measures in place for each information asset. This should help ensure security measures are consistent across the organisation.

✓ Another agency hired an external organisation to carry out a data protection/information security audit in order that areas of weakness and risk could be identified and addressed.

✓ Data protection/information security issues are kept high profile within one organisation as they are reported as a standing item at each senior management team meeting.

More information

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

- Data protection guidance
- Training checklist for small and medium sized organisations
- A practical guide to IT security (pdf)
- Employment code of practice – quick guide (pdf)
- 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**.