# Findings from ICO advisory visits to social housing organisations

February 2014

# Contents

# 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 nine advisory visits to social housing organisations to get 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 where the 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.

Since 2011 the ICO has also undertaken four audits of social housing organisations. Audits are aimed at larger organisations that have the basics in place but are looking for assurance that their policies and procedures are working in practice. The audits normally look at defined scope areas, such as governance, subject access request (SAR) handling, records management, and result in a detailed report.

Local authorities (LA) have a statutory duty to create a housing strategy to meet housing needs. This responsibility is usually shared with housing organisations that act for or on behalf of LAs. As part of our work we therefore visited both housing associations and arms-length management organisations.

## Housing associations (HAs)

HAs own and manage social housing. They are usually not for profit organisations run by voluntary boards.

Many HAs are independent Registered Providers but can be subsidiaries or members of larger groups. Groups vary and can contain a mix of other smaller groups, private companies, HAs and charities.

## Arms-length management organisations (ALMOs)

ALMOs are created and owned by LAs and work under contract to autonomously manage, maintain and improve LA housing stock. The LA owns the housing stock, responsibility for housing strategy, housing benefit and rent policy.

ALMOs must collect rents, manage arrears and debt counselling and arrange lettings. They must also encourage tenants to work as partners in estate management and be able to demonstrate continuous improvement of tenant services.

The housing organisations we visited varied considerably in terms of the numbers of staff, the resources and facilities available to them and the sophistication of their systems and processes. However, due to the nature of the work they carry out, they also had many commonalities.

This report highlights our experience of personal data handling by social housing organisations and is intended to help these organisations see where they can make improvements in how they handle their personal information and also inform other organisations who are processing personal data in similar circumstances.

## Typical processing of personal data by HAs

Housing organisations process information about their tenants in paper and electronic form. As well as general contact, tenancy and financial information this can also include sensitive personal data especially where they are involved in providing assisted housing for example, for people living with a disability, elderly or vulnerable people.

While our work focussed on HAs and ALMOs we believe that many of the issues highlighted in this report are equally relevant to other organisations in the housing sector, for instance private rental companies and landlords.

# Challenges and remedies

Through working with housing organisations we were able to gather information about the challenges and good practice remedies that were in place. Below are the key findings from our visits. These are provided in order of the frequency they were encountered.

## 1. Data sharing agreements

Housing organisations often have a requirement to regularly share personal data with other organisations. Often this is in relation to normal course of business disclosures such as maintenance contractors. But it may also include information that needs to be shared, for instance, in order to chase unpaid bills, or for legal proceedings where property is damaged. Unfortunately, they tend not to have formal policies and procedures to mandate that sharing.

By implementing formal data sharing arrangements a housing organisation can:

- stipulate when information can be shared;
- ensure requirements for dealing with subject access requests or, where applicable, freedom of information requests are specified;
- specify what security measures need to be in place;
- limit who is allowed to sign off data sharing; and
- require records of sharing to be maintained.

Establishing formal agreements with organisations sharing data allows housing organisations to mandate how the information will be processed over its lifecycle, including how it is disposed of. Reviewing these agreements regularly ensures they continue to meet the housing organisation's requirements.

## Did you know?

We've produced a statutory data sharing code of practice, which is available on the ICO website at:

http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

## 2. Retention schedules

Housing organisations often do not have formal retention schedules in place for personal data. Under data protection legislation, organisations should not hold personal data for longer than necessary.

Where there are retention schedules implemented they are often only applied to physical records. Good examples of retention schedules and associated policy:

- specify who is responsible for destroying records;
- justify the retention of records based on the type;
- set out how any exceptions to retention schedules are applied and reviewed;
- list appropriate disposal methods and security requirements;
- apply to both electronic and manual records;
- set out the requirements for recording records as destroyed; and
- implement checks to ensure the retention schedule is applied.

### Case study - applying retention schedules.

Housing organisations work with vulnerable adults and children. As a result key staff undergo a criminal records check for their role. The retention requirement to hold this sensitive personal data is different from other information (for example, payroll information) held on the HR file.

By recording only that a check had taken place and there was no disclosure that would bar employment, housing organisations are then able to dispose of the disclosure material.

# Did you know?

Applying retention schedules to personal data is a legal requirement under the Fifth Principle of the Data Protection Act 1998. Guidance is available on the ICO website at:

http://ico.org.uk/for_organisations/data_protection/the_guide/information_standards/principle_5

## 3. Encryption of portable devices

Portable devices that store personal data (for example laptops, USB sticks and DVD/CD media) pose a high risk to data security. The Information Commissioner believes that portable devices that store personal data should use encryption to protect the information. Enforcement action taken by the Information Commissioner is often in relation to organisations failing to encrypt personal data stored on portable devices. Since 2010 the ICO has issued nine civil monetary penalties totalling £895,000 in cases where personal data held on portable devices was not encrypted. While many of the housing organisations we visited implemented encryption methods to protect personal data, not all did so.

### Case study - forcing USB encryption.

At one of the housing organisations there were technical solutions in place to force encryption. The system only allowed encrypted information to be copied to approved USB devices. Logs were generated of information copied to portable devices and any attempts to copy information to a non-approved USB device this would be recorded and highlighted.

# Did you know?

For more information about our approach to the use of encryption to enhance the security of personal data we have guidance on our website at:

http://ico.org.uk/news/current_topics/Our_approach_to_encryption

## 4. Remote working

Although not all the housing organisations visited have remote or homeworking available, where it was used it often wasn't formalised.

Documenting a policy for remote or homeworking allows the housing organisation to stipulate:

- when remote or homeworking is appropriate;
- technical controls for the security of personal data used;
- staff responsibilities;
- procedures for authorising remote or homeworking; and
- when and how often remote working will be reviewed.

### Case study - planning for the worst case scenario.

Remote and mobile technologies are becoming more prevalent in all organisations. They allow greater opportunities for flexibility which organisations are keen to take advantage of. They also offer opportunities to improve security over manual records by restricting access to information. However, there are also increased risks resulting from:

- the capacity to carry large volumes of personal data; and
- electronic devices being more likely to be targeted in opportunistic thefts than a manual record.

One of the housing organisations had an additional measure in place to further increase the security of portable devices. As well as being encrypted and password protected, they also had kill codes. This meant that in the event of the device being lost or stolen, the housing organisation could wipe the information remotely.

# Did you know?

With the more staff and volunteers now using their own devices the ICO has produced bring your own device (BYOD) guidance that is accessible from our website at:

http://ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

## 5. Training

There were varying levels of data protection training in housing organisations. Training is a key tool for any organisation in ensuring that staff are aware of their responsibility for data protection.

Key elements of good practice for data protection training include:

- mandatory induction training that ideally takes place before allowing staff to access personal data;
- mandatory annual refresher training;
- annual reviews of data protection training content to ensure that it is up to date and remains relevant to the housing organisation's needs;
- specialised training for key roles, for example those dealing with requests for personal data, information security, or records management;
- training records that record completed data protection training; and
- procedures to ensure that incomplete training is chased up and resolved.

# Did you know?

We've produced tools to help organisations deliver training to their staff. This freely available material can be accessed on our website at:

http://ico.org.uk/for_organisations/training

## 6. Physical security

By preventing unauthorised access to premises, organisations reduce the risk of unauthorised access to personal data. There were good practice examples that housing organisations had in place in relation to physical security. These included:

- staffed reception;
- ID badge requirements for staff and visitors;
- swipe card access; and
- dedicated areas to meet confidentially with customers and members of the public.

### Case study – zone restricted access.

By using employee swipe cards organisations are able to restrict access based on role. For example, only designated employees are able to access the cash office, or server rooms.

One of the housing organisations that we visited used this to restrict access to certain times. For example, employee swipe cards would only allow access during their contracted hours, thereby preventing access for part time staff on their non-work days.

## 7. Secure printing

A secure printing solution can reduce unauthorised internal access to personal data. It can also reduce the risk of sensitive printed material being bundled incorrectly and mailed to the wrong address. Therefore, such solutions provide greater assurance that paper records are processed in accordance with data protection requirements for security. Many of the housing associations visited did not implement these solutions.

Where good practice was evident this included pin-coded printing or swipe cards being in place to access devices. As housing organisations look to refresh old hardware they should consider these devices as a strong measure for improving security.

## 8. End point controls

Access to USB ports and DVD/CD drives pose a significant risk to the security of personal data. These portable media solutions allow large amounts of personal data to be removed immediately, as well as allowing the transfer of malware onto the organisation's systems. There were examples where housing organisations had not restricted this access.

By locking down the use of USB ports and DVD/CD drives, housing organisations can mitigate the risk of loss on a massive scale and the transfer of malware. Where access is allowed it is good practice to;

- restrict the access to roles where it is required;
- ensure access is signed off and recorded;
- only allow access for a set period of time; and
- regularly review access to ensure it is still required or has been removed.

### Case study – thin client advantages.

By removing the hardware that can be used to copy large amounts of personal data onto USB sticks and DVD/CDs, organisations can limit their exposure to this risk. One of the housing associations had implemented a thin client solution for their staff.

This meant that the traditional PC setup had been replaced with a simple connection box which did not provide staff with access to DVD/CD burners or USB ports.

## 9. Role based access

Restricting records access to only those that require the information to work helps protect individual privacy. For example, someone working in payroll may need to access financial information about staff, but wouldn't need to access sensitive housing records. Conversely, staff working with housing clients would not need to access another employee's payroll data.

Housing organisations visited demonstrated good practice in relation to role based access for their systems. Access was aligned to the role requirements of employees and prevented access to non-relevant personal data.

### Case study – particular restrictions.

Modern IT systems often provide an opportunity to restrict employee access to particular groups of records. For example, only allowing access to records that are relevant to their team or that have been assigned to them. One of the housing organisations that we visited put additional restrictions in place. As many of their staff are also part of the community they are required to disclose any links (for example, relatives) they may have with the housing organisation's clients. The system is then locked down to prevent the staff member from accessing those particular records.

## 10. Monitoring

Policies and procedures help maintain requirements and standards for organisations. By monitoring a policy or procedure's effectiveness organisations are able to gain assurance that they are having the desired impact. During our visits there was little evidence that housing organisations had this monitoring in place.

For example, some housing organisations had clear desk requirements in place, but did not perform regular checks to ensure staff compliance. The results from checks highlight any problems, for example in staff awareness, which can then be addressed.

When policies or procedures are new there are more likely to be issues with how they are implemented. By monitoring new policies and procedures housing organisations can ensure they are embedded adequately.

## 11. System access

Having controls in place to ensure that access to systems is restricted reduces the opportunities for inappropriate access to personal data. There were housing organisations that we visited where adequate access controls were not in place.

Good practice implementation of access controls:

- restrict access based on role (see role based access);
- ensure that access is reviewed on a regular basis;
- update access accordingly when an employee changes roles to ensure they do not accrue access rights that are not required;
- remove system access promptly once an employee leaves an organisation; and
- have procedures for removing access promptly if an employee is suspended or dismissed.

### Case study – promoting leaver communication.

Ensuring that access to systems is removed promptly once staff leave is a key requirement for any organisation. Often it can rely on managers informing IT departments that account access needs to be blocked. One housing organisation that we visited took an extra step to promote the communication of this information. Until the line manager had supplied the leaver's form the recruiting of a replacement would not be authorised.

## 12. Password requirements

Passwords provide a way to restrict access to systems. Although all housing organisations visited had password requirements for their systems, there are key elements of good practice that can be implemented to maximise this security measure.

- Ensure that staff have a unique account and their own logon - this also helps with the integrity of audit trails.
- The system forces a regular change of passwords to reduce the impact of a password being discovered.
- Force passwords to be over a certain length and contain a combination of numbers, characters and different case letters.

## 13. Records inventory

By having a comprehensive records inventory in place, organisations have a clear view of what they are processing and are better able to manage records effectively. The housing organisations visited often failed to maintain such an inventory.

Key elements of an effective records inventory include:

- what records are held;
- what they contain;
- information about the format of the record;
- applicable retention schedules (see section 2);
- the purpose for which they are held; and
- who is responsible for their management.

## 14. Fair processing information

To process personal data organisations are legally required to advise individuals how their personal data will be used. It is also good practice to tell people how they can access any personal data that is held.

While there were varying standards across the housing organisations visited for providing this information, there were examples of good practice. These included:

- standard information for use on forms;
- scripts to ensure the information can be communicated verbally; and
- copies of the fair processing information made available on the housing organisation's website.

# Did you know?

Further information about privacy notices which are used to provide fair processing information to individuals is available on our website at:

http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices

## 15. Staff awareness

Awareness raising measures can help an organisation increase staff knowledge of their data protection obligations. This in turn should improve compliance with data protection. There were two notable areas of good practice from the housing organisations that we visited in this regard.

- Posters were used around the housing organisation's offices to highlight key data protection and information security issues.
- Staff were required to sign to say they had read and understood policies which included data protection and information security.

### Case study – further awareness.

Through the use of multiple methods to promote data protection, organisations can increase staff awareness and target specific issues. As well as a poster campaign, one housing organisation that we visited included data protection issues in weekly team briefings and sent out leaflets with payslips.

# Did you know?

The ICO has produced tools to help organisations of all sizes make their employees aware of their data protection responsibilities. The 'think privacy' toolkit is available on our website at:

http://ico.org.uk/for_organisations/training/think-privacy-toolkit

## 16. Data protection leadership

Having a data protection lead helps drive compliance throughout the organisation. Most housing organisations did not have a data protection lead.

Having a lead for data protection has most positive impact if they:

- are at board level or report directly to the board;
- have oversight (for example, through monitoring) of compliance;
- sign off on any information governance requirements for the annual statement of assurance or equivalent; and
- are able to drive any changes required for better data protection compliance.

## 17. Fax machines

The Enforcement action the ICO has taken indicates that fax machines represent a significant risk to organisations. Fax machine usage is becoming less common in organisations, but even rare usage represents a risk. Use of fax machines by housing associations was low and often only required where organisations they dealt with did not have another communication solution. However, their ongoing use means that the risk of wrongly disclosing information should be considered and mitigated.

By implementing a fax usage policy housing organisations can reduce the risk. Where faxes are used it is good practice to:

- require a pin or swipe card for access;
- have pre-programmed numbers to prevent misdialling;
- limit the number of machines;
- restrict the information (for example, limit the amount of personal data) allowed to be sent;
- require the receipt of a test page to be confirmed before sending through information; and
- require confirmation of receipt of information so that any losses can be identified and investigated quickly.

Removing fax machines and preventing their use in favour of secure electronic transfer solutions is better practice.

## 18. Data protection policies

The use of formal policies and procedures is essential for any organisation to ensure compliance with data protection requirements. There were a number of housing organisations that demonstrated good practice in relation to management of these policies. This included policies:

- having clear owners;
- being reviewed annually;
- having version numbering to ensure the latest version could be identified; and
- being promoted, with any training needs they raise being identified and implemented.

### Case study – policy review triggers.

In order to ensure that policies and procedures are still fit for purpose it is essential they are reviewed regularly. One of the housing organisations that we visited used policy management software that triggered reminders before a policy review was due.

# Additional challenges

Each of the housing organisations visited were eager to work with the ICO to improve their compliance with the Data Protection Act 1998 (DPA). They had already considered their requirements and had put measures in place. However, intelligence from ICO casework reveals that not all housing organisations are taking adequate measures to ensure that they comply.

Where housing organisations do not implement adequate measures to comply with the DPA they could face enforcement action by the ICO. For serious breaches of the DPA this may result in a civil monetary penalty of up to £500,000.

While this document highlights the key challenges and remedies that housing organisations should consider it is not an exhaustive list. Housing organisations must be aware of the risks and requirements involved in processing personal data and ensure they implement adequate measures to deal with these.

As well as the information that we were able to gather during our visits to housing organisations we also have intelligence from our complaints casework and our strategic stakeholder liaison activities. There are two other areas of concern that we would like to highlight.

## 19. Subject access requests

Under the DPA individuals have a right to obtain copies of their personal data that organisations hold. Upon receipt of a valid request a housing organisation must ensure they respond within 40 calendar days.

## Did you know?

The ICO has produced a subject access code of practice for organisations which provides practical advice for dealing with requests for personal data. It is available on our website at:

http://ico.org.uk/for_organisations/data_protection/subject_access_requests

## 20. Accuracy of personal data

The DPA makes it a legal requirement for organisations to ensure that the personal data they process is accurate and, where necessary, kept up to date. Where housing associations are processing personal data, often to deliver essential services to vulnerable people, it is vital that the information is accurate.

# Did you know?

Further information about keeping personal data accurate and up to date is available on the ICO website:

http://ico.org.uk/for_organisations/data_protection/the_guide/information_standards/principle_4

# More information

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

- Data protection guidance

Other useful guidance:

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

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

In 2009, Orbit Housing Group reported a data loss incident relating to a number of tenant's files. As well as implementing measures to improve how they handled personal data, they also produced a video with the ICO to show what went wrong and what steps they took to improve their practices.

The video is available to view on the ICO training and information video page:

- ICO training videos

# Further assistance

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