ico.

Information Commissioner's Office

Findings from ICO advisory visits to nurseries

February 2018

Executive summary

The Information Commissioner’s Office (ICO) enforces and promotes compliance with the Data Protection Act 1998 (the DPA), which contains eight principles of good information handling. The ICO will maintain an equivalent role in respect of the General Data Protection Regulation (the GDPR), which will take effect in the United Kingdom from 25 May 2018.

The ICO’s Assurance Department is responsible for promoting good practice in relation to personal information handling. We undertook a project looking at private and state funded nurseries to help the sector improve its data protection compliance. We chose nurseries as a focus sector due to the vast number of links nurseries have with local government; the sharing of personal information with other organisations such as social care services; and the often limited resources nurseries have available to dedicate to data protection compliance.

Approach

During 2016 and 2017, 11 data protection advisory visits were carried out at nurseries across England, Scotland and Wales.

Advisory visits take place over one day and are a free and informal way for the Assurance Department to provide practical advice and guidance to small organisations on data protection compliance. They focus on security, records management and requests for personal data. A short report is produced and provided to the organisation, which highlights areas of good practice and areas for improvement.

The nurseries for this project were selected by approaching larger nursery chains’ head offices and also by looking at the previous contact nurseries have had with the ICO. Contact with the ICO included: seeking advice, reporting information security incidents or responding to the ICO regarding complaints received from members of the public.

This overview report identifies the common themes and trends identified during the course of these 11 advisory visits. We hope this will help nurseries improve their data protection compliance.

Typical processing of personal data by nurseries

Nurseries process both paper and electronic records relating to children in their care, their parents/guardians and members of nursery staff.

Nurseries process a limited amount of sensitive personal data, including health information relating to the children in their care and staff sickness records.

Other information typically held includes: names, contact information, financial information, children's likes/dislikes and behaviour, whether the parent/guardian is in receipt of tax credits, whether the parent/guardian is claiming free nursery care from the local council and attendance lists.

Personal information is either held electronically in computer databases or manually in filing cabinets.

Areas of good practice

In most nurseries we visited we noted that:

- ✓ A data protection policy, confidentiality or related policies were in place and these were reviewed regularly. In most cases, employees also had to read and sign to confirm that they understood the content of nursery policies. Additionally, the policy was regularly discussed during discussions with staff at team meetings or 1-2-1 sessions.

- ✓ Robust physical security measures were in place at the majority of nursery sites we visited, which consisted of either fingerprint entry systems, intercom/buzz entry or entry based on prior agreement with the nursery. All visitors also had to sign in at reception and were accompanied at all times by a member of nursery staff, which is good practice.

- ✓ The majority of nurseries we visited had either cross cutting shredders to destroy confidential waste, or they used a third party company to remove and securely destroy their confidential waste.

- ✓ All nurseries we visited gained specific consent for taking photographs of children and sharing personal information with other organisations, where this was required. Under the GDPR, consent is one of six available lawful basis for processing personal data. Organisations need to identify one of these lawful basis before they start processing.

- ✓ Some of the nurseries we visited had CCTV in operation. The footage was held securely and reasonable retention periods were in place for the footage, in line with the ICO's CCTV code of practice.

- ✓ Fair processing information was made available to individuals at the time personal data was collected. To ensure that personal data is processed fairly, individuals need to be told about how their personal data will be used, which is usually communicated in the form of a 'privacy notice'.

Areas for improvement

In most nurseries we visited we noted that:

- Bespoke data protection training was not in place for staff. Training staff on their obligations under data protection law, is vital to protect personal data and to aid in preventing security incidents involving personal data. The ICO recommends that all staff complete data protection training on induction and **at least** every two years throughout their employment. We have a number of resources available on our website to help design and deliver training.

- Processes for reporting and investigating security incidents involving personal data were not documented. It is important that organisations have a documented and embedded procedure for managing security incidents involving personal data, to reduce the risk of harm to affected individuals and ensure appropriate escalation. All staff should be told how to recognise a security incident and how to report them.

- A process for dealing with subject access requests was not documented. Making a subject access request is one of the key rights afforded to individuals in data protection law, so it is important that nurseries understand how to recognise a request and process a request.

- Nurseries did not always have a data sharing policy in place, which explained the circumstances in which they would share personal data with third parties. Additionally, if information was shared, this was rarely documented. There are a number of circumstances in which the law may permit the sharing of personal data with other organisations, however, there should be a clear documented process in place for deciding when and if personal data can be shared. This must be appropriately documented to ensure accountability.

- A documented retention schedule for personal data was not always in place. Additionally, regular weeding, archiving and destruction of paper or electronic records did not always take place. Data protection law requires that personal data is not retained for longer than is necessary. In practice this means an organisation should have a documented retention schedule in place which takes into account any legal or regularity requirements, agreed industry practices and the specific circumstances regarding the personal data.

- USB sticks and laptops were not always encrypted and in nurseries where USB sticks were not used, USB ports were not always locked down. The ICO strongly recommends that all portable devices, which contain personal data are encrypted. The ICO's guidance on 'encryption' provides detailed guidance on this.

In some of the nurseries we visited we noted that:

- Staff often shared login information and passwords, rather than having their own individual profile for electronic case management systems and other applications. Sharing passwords and login information means that appropriate access controls are not created and additionally, an accurate audit trail of access, amendment and deletion of records cannot be maintained.

- It was unknown whether anti-virus and firewall protection was always kept up to date or whether endpoint control was utilised. This creates an obvious risk to the nurseries personal data as it could enable unlawful access to personal data and delay detection.

- Passwords on electronic devices tended to be weak and were not changed regularly enough. Additionally, devices did not automatically lock after a period of inactivity.

- Secure printing was not always used or available. Where secure printing was unavailable, printers were not always kept in secure areas, or prints were not collected immediately from the printer. This could mean documents containing personal data could be inappropriately disclosed to other members of staff, or be misplaced.

- Where remote or homeworking was permitted, there was no documented policy or procedure to advise staff of their obligations, such as, taking electronic equipment and paper records offsite. It is vital that personal data taken outside of the office is awarded the same level of protection if it is taken outside of the office. This is also the case if organisations allow members of staff to use their own devices to carry out the work of the organisation. The ICO's 'bring your own device (BYOD)' guidance will be helpful when designing a remote working policy or guidance for staff in this area.

- If third party organisations were utilised for services such as; record disposal, hardware disposal and IT services, contracts were not in place, or it was unclear whether these contracts included appropriate security clauses to protect the personal information that was accessed. If a third party is involved, an organisation needs to ensure that the third party affords the same level of protection to personal data as they do. In particular, ensuring that data is not accessed or used without their agreement.

➔ Paper files were not always stored securely when not in use during the day. After closing time, paper files were normally stored in lockable filing cabinets, however, these were not always locked, or the keys to the cabinets were not stored securely. If paper records are not stored securely when not in use, they may be misplaced, or lost, therefore it is advisable to have a clear desk policy in place. Paper files should be stored in lockable cabinets, with keys securely stored- ideally in a key coded wall safe.

➔ If a fingerprint entry system was used to allow access to the premise, it was not always clear whether appropriate, storage and retention periods were applied to this information. A fingerprint entry should be removed from the system as soon as an individual withdraws from the nursery, which should include parents/guardians, nursery staff and anyone else with access.

More information

The ICO has produced guidance which can help nurseries look after personal data and comply with changes to data protection law. This information can be found on our website and includes:

- Guide to the GDPR
- Getting ready for the GDPR checklist
- GDPR FAQ document

Further assistance

The ICO also has a helpdesk with staff on hand to answer queries about data protection compliance; they can be contacted via telephone, live chat or email at: ico.org.uk/global/contact-us