Portsmouth CITY COUNCIL

Data Protection including Subject Access Requests and the Data Security & Protection Toolkit

Sam Midgley
Information Governance Lead in Adult Social Care

Data Protection law

- Data Protection Act 2018
- UK GDPR (General Data Protection Regulation) came into effect from 1 January 2021.
- Common Law duty of confidentiality

They apply to personal data and special categories of personal data which are subject to more stringent conditions for processing. Information relating to a person's care needs will be special category personal data.

There are six legally enforceable principles of good practice under the Data Protection Act which we will look at in turn.

Every organisation should have someone who leads on data protection.

Principle 1: The processing of personal data is lawful, fair and transparent.

- We must only process data where there is a legal basis for doing so
- If no legal basis exists, we can process data if we have the explicit and freely given consent of the data subject or their representative
- Personal data is shared when appropriate
- Data subjects can exercise their rights, for example to rectification of errors and to be informed what their information will be used for

Principle 2: Data is used only for the purpose it was collected for

- The purpose for which data is collected must be specified, explicit and legitimate
- Data must be processed in a manner that is compatible with that purpose

Principle 3: Personal data collected is not excessive

- Data must be relevant for the purpose for which it is being processed
- Data must be adequate for the appropriate business process to be carried out effectively but not exceed what is required

Principle 4: Personal data is accurate

- Data is kept up to date and is of good quality
- This is vital to ensure the right decisions can be made based on the right information
- Systems must be kept up to date, whether they are paper or electronic and must give a clear and accurate picture which is unambiguous

Principle 5: Personal data is kept for no longer than is necessary

- Organisations need a retention schedule which states how long different files will be retained
- Data must deleted in line with the retention schedule
- There must be a clear business reason for keeping information and not retaining it indefinitely “just in case”

Principle 6: Personal data is processed with appropriate security measures

- All staff must be trained and have regular refresher training
- Someone in the organisation should be responsible for data protection and able to give advice to staff
- Appropriate technical and organisational security measures are in place to safeguard data
- Data Protection Impact Assessments are carried out for any processing that is high risk
- Data processing is regularly audited and compliance concerns are acted upon
- Papers files are kept in a secure environment

Principle 6 continued

- The organisation has a data in transit policy to outline expectations when papers are taken out of the office
- Any data breaches are reported and acted upon swiftly to follow up and identify if they need to be reported to the Information Commissioner's office
- Staff receive advice from the organisation's IT security staff and are clear what is required of them to keep IT secure and legal
- Staff are aware that they only access personal data where there is a business need for them to do so
- Staff never access the records of clients they know personally but flag with a manager who will ask someone else to work the case

Data Subject Access Requests (DSARs)

- By law, people can ask for a copy of any information held by an organisation about them as it is their personal data
- When a request is received, the identity of the person must be checked to ensure the files will be sent to the data subject or an appropriate representative
- In terms of requests by someone who is not the data subject, consider the client's wishes, whether the person is involved regularly in the client's care and whether there is a Power of Attorney in place for Health and Welfare

DSARs continued

- Once the request is received, you have one calendar month from when the ID check is completed to send the information out
- Clarify what information is required- there may be a specific time period of interest and the whole file may not be required
- Redact any information that does not relate to the data subject
- You may need to balance the rights of two people when deciding what to redact, eg the privacy rights of one person v the rights of another person to know what happened. Get advice if you are unsure what to do

DSARs continued

- The Information Commissioner's Office website provides a step by step guide for small organisations when dealing with a DSAR https://ico.org.uk/for-organisations/advice-for-small-organisations/

What is the Data Security and Protection Toolkit

- This is self assessment tool
- Organisations measure their performance against the National Data Guardian's data security standards by answering a series of questions which reflect the situation in their organisation
- Care providers need to answer 42 mandatory questions relating to Staffing and roles, Policies and Procedures, Data Security and IT systems and devices
- The Digital Care Hub provides detailed guidance for care providers on how to reach standards met on the DSPT: https://www.digitalcarehub.co.uk/dspt/

Any questions….