Records Management

Scope: The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

Risk: In the absence of appropriate Records Management processes, there is a risk that records may not be processed in compliance with the GDPR and other national data protection legislation, resulting in regulatory action by the Information Commissioner's Office, reputational damage to the data controller and/or damage and distress to individuals.

Domain	Control	Control measure
RM Organisation	There are appropriate organisational arrangements in place to support the records management function. There are defined roles and clear lines of responsibility assigned.	Lead responsibility for the strategic direction and oversight of RM has been assigned to an executive board member (e.g. SIRO).
		Operational responsibility for the development and implementation of the RM function has been assigned to a corporate Records Manager.
		Local responsibilities have been assigned to ensure the RM policy is implemented within business areas e.g. IAO, IAA etc
		A steering group meets regularly to mandate and monitor RM improvements.
		There is a RM policy in place, which is subject to senior management approval and periodic reviews to ensure it aligns with the latest guidelines.
		RM is incorporated within a formal training programme and good records management practices are promoted across the organisation.
Collection of data	Individuals are informed about the use of their personal data.	Fair processing is understood by staff and actively communicated to individuals in line with the ICO's Privacy Notices Code of Practice and the requirements of the GDPR.
		Fair processing information is presented in a language and format which is readily understandable and accessible.
Creation of records	When creating documented information the organisation has ensured there are appropriate identification, classification and security measures	Appropriate identification, security classification, description and format has been assigned to new information / records (or information added to an existing record or file).
		Appropriate access levels have been assigned to any new information / records (or information added to an existing record of file) on creation / collection.
Storage of records	An inventory of paper and electronic records is maintained.	There has been an information audit across the organisation or within particular business areas to identify the data processed and how it flows into, through and out of the organisation.
		A comprehensive inventory or asset register is in place and maintained that shows what records are held, what they contain, in what format, and what value they have for the organisation.
	Access is controlled to storage areas for paper based records and they are regularly inspected.	Appropriate access controls are in place to mitigate the risk of unauthorised access to physical records
		Periodic audits are carried out to assure the security of 'in-house' records storage.
		Where semi-current paper based records are stored by a contractor the organisation has established the right to periodically visit their premises.
	There are effective mechanisms in place to locate and retrieve physical records on demand.	The whereabouts of records are known at all times and the movement of records between storage and office areas is logged and tracked to facilitate control and provide an audit trail of all record transactions.
		Attempts are made to trace records that are missing or not returned to storage in a timely manner.
		Records stored off-site are indexed with unique references to enable accurate retrieval and subsequent tracking.
		Compliance checks are undertaken to assure the effectiveness of tracking mechanisms.
Maintenance and accuracy of records	There are procedures in place to ensure the adequacy, integrity and accuracy of information, and that it is not excessive for the purposes.	There are procedures in place which allow individuals to challenge the accuracy of the information the organisation holds about them and have it corrected if necessary. Where the inaccuracies are unable to be rectified procedures dictate that the inaccuracy is documented.
		Where inaccuracies in data that is shared with 3rd parties has been identified, there are procedures in place to ensure the 3rd party is informed in a timely manner.
		There are regular data quality reviews of systems and manual records created, processed or stored to ensure the information continues to be adequate for the purposes of processing (for which it was collected).
		Staff are made aware of data quality issues both through ongoing awareness campaigns or training, and following specific data quality checks or audits.
		Information or records (both 'active' records and records in archive) are weeded on a periodic basis to reduce the risk of inaccuracy or excessive retention.
	There is a retention schedule outlining storage periods for all personal data(this includes manual and electronic records) which is reviewed regularly and has a designated owner.	The organisation has produced a retention schedule based on business need with reference to statutory requirements and other principles e.g the National Archives. The schedule provides sufficient information for all records to be identified and disposal decisions put into effect.
		The retention schedule is regularly reviewed to make sure it continues to meet business and statutory requirements and any amendments are agreed with managers are incorporated into the new schedule
		Responsibility for retention and disposal is designated to an appropriate person (this could be centrally or in each department e.g. IAOs)
		Records are disposed of in line with the Retention Schedule
		There is evidence of management sign off / approval prior to disposal of records
	Methods of destruction are appropriate to prevent disclosure of personal data prior to, during and after	For paper documents cross shredding or incineration either in-house or by a third party is in place.
		For documents / information held on electronic devices; wiping, degaussing or secure destruction of hardware (shredding) is in place.

Disposal of records	disclosure of personal data prior to, during and after disposal	Confidential waste is controlled through policies and secured collection. Equipment awaiting disposal is held in a secure area and there is an inventory of devices awaiting disposal.
	If third parties are used to dispose of personal data there should be a contract in place that includes the requirement to have appropriate security measures in compliance with DPA and the facility to allow audit by the DC.	Contracts are compiled by the appropriate people and contain the necessary DP legal requirements/clauses (that include security requirements and the ability to audit by the DC).
	If third parties are used to dispose of personal data the persons with responsibility for retention and	Occasional checks are being made on third parties to ensure security is of the appropriate agreed standard
		Nominated staff are obtaining destruction certificates that correspond with the amount of paper waste or equipment that has been sent for destruction.
	There are procedures in place to provide individuals with the 'right to be forgotten' (under the GDPR).	There are procedures in place which allow individuals to request the deletion or erasure of their information the organisation holds about them where there is no compelling reason for its continued processing.
		Where the organisation has deleted or erased an individuals information and that data has been shared with 3rd parties previously, there are procedures in place to ensure the 3rd party is informed in a timely manner.