Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status
Requirement to have a Data Protection Officer (DPO)	No requirement to have dedicated staff assigned to managing data protection.	Art. 37-9: Define the new requirements for DPO. The DPO shall have expert knowledge of data protection law and practices, and must report directly to the 'highest management level of the data controller' A DPO is required if • Public authority • Carry out large scale/systematic monitoring of individuals • Carry out large scale processing of special categories	The legal role of DPO will be held by the Council's SIRO (Director of Governance) however consideration should be given to the need to appoint a specialised role to ensure the transition to GDPR is completed and that ongoing adherence is managed. On the basis of this, it would suggest good practice for the Fund to have a DPO given the amount of personal and sensitive data it holds and for the Head of Governance to be given this responsibility.	ASAP	The council's Director of Governance holds the position of Senior Information Officer for the Fund, however for the purposes of GDPR the Head of Governance has taken the responsibilities for the Fund.
Awareness		Greater level of responsibility in ensuring compliance of the fund but also ensuring compliance of third party contractors.	Staff briefings to be held on new requirements outlining key responsibilities and penalties. Regular updates to the Pension Board and the Pension Committee on the progress of work	February 2017 To be reported on each meeting as part of the quarterly compliance monitoring program	

Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status
		Greater public awareness of their rights under GDPR.	Staff briefings to be held on new processes once drafted	June 2017 .	
			Presentation to employers at AGM.	November 2016	Completed
Information audit (Data Discovery) • Identify what data is held • Where it came from • Who it is shared with	Applies to personal data	GDPR's definition is more detailed and includes 'identifiers' (could include pension reference number).	Ensure the pension reference number is afforded the same protection as personal data – staff to be retrained on this.	Staff Briefings February and June 2017	Ongoing discussions with software supplier
		Adds a new accountability requirement requiring authorities to show **how** they comply with the principles through documenting decisions which are taken about a processing activity. Not enough to take the decision, must show the process of the decision.	Review of all processes to ensure they are documented with published process maps showing how information is used and trail its use through the fund from joiner to leaver/retirement/death.	By January 2018	List of processes identified
		Information must be collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with	Review all third party contracts to ensure compatibility with this principle. Consider who we share information with and in what form (identifiers now fall	By April 2017	Under review by compliance as part of a wider contract review program.

Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status
		that purpose.	under GDPR) seek assurances on use.		
		Adequate, relevant and limited to what is necessary	Data cleanse project to review information held (see below). Identify processes and where information is collected Review periodically information held and consider whether needs to be updated (e.g. deferred members with ex-husbands/ill health retirement and medical records no longer required).	Commence January 2017 Commence January 2017	Meeting to be held with all team managers in January to discuss resources and project group.
		Accurate and kept up to date, every reasonable step must be taken to ensure that personal data that is inaccurate is rectified or deleted	Data discovery exercise to identify duplicate records which may hold different information, work with employers (monthly returns) to ensure information being received is accurate. Use of web portal (needs	Commence January 2017 Commence	Meeting to be held with all team managers in January to discuss resources and project group.

Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status
			marketing push) to help members self-serve and rectify errors.	marketing February 2017 and throughout the year	
		Processed in a manner that ensures appropriate security	Discussions with Civica to ensure they are up to date with GDPR and the obligations on them. Seek assurances of their processes. Discussion with WCC ICTS (already in progress with WCC IG team).	ASAP but need assurances by January 2018	Discussions started
Information Audit (Data cleanse)	Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. Personal data	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; Adequate, relevant and	As a data processor the Fund needs to ensure that all the data we hold is held for a valid reason and to perform a specific function. (holding onto medical records after a decision has been made and in excess of any appeal period would be deemed to be a breach of the GDPR as the Fund will no longer need the information to pay the pension benefit. Such information should be returned or destroyed). The responsibilities in this	To be completed by January 2018.	Reports to be run on UPM to identify where numerous records are held for one member The Fund is

Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status
	shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Personal data shall be accurate and, where necessary, kept up to date.	limited to what is necessary in relation to the purposes for which they are processed; Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;	area haven't changed much from the DPR, however the greater transparency requirement and the rights of individuals means the Fund will be open to greater scrutiny about the information it holds and it should therefore ensure that all the information is held for a valid reason. Furthermore the Fund has a duty to document its processes for managing data and removing inaccurate or unnecessary data will assist with this transparency.		reviewing the information it places on the website to inform members about how their information is held. Also looking into pop-ups on the web portal facility.

Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status
Third party contracts	Responsibility of processors limited	Greater responsibility on processors to ensure compliance and greater responsibility on controllers to ensure their compliance and seek assurance of compliance.	Review all third party contracts for data protection clauses and re-draft with GDPR Get assurance from third parties of their adherence to GDPR Re-draft data sharing agreement	ASAP	Contracts identified letters to be sent in January 2017.
Children's Data and beneficiary members		GDPR contains provisions intended to enhance the protection of children's personal data and requires that privacy notices are written in a manner that children will understand	Review information provided to child pensioners and ensure complies with GDPR	ASAP	
Privacy Impact Assessments	Requirement to give certain people information such as identity of Fund, and how we intend to use the information	Under GDPR, there is additional information which needs to be provided. • Legal basis for processing data • Data retention periods • Right to complain	ICO has published a code of practice for conducting Privacy Impact Assessments. All processes conducted by the Fund need to be individually assessed under this Code to ensure compliance with the PIA published on the Fund's website.	ASAP completed by January 2018	

Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status
Privacy Notices	We must inform data subjects of the processing of their data we will undertake and the purposes for that processing.	Details much more precisely how data subjects should be informed about the processing of their personal data (at the time their data are obtained)	Need to review policies and publish them on the website	ASAP	
Individual's rights		Right to rectification of data	Fund will need a process for accepting these requests with adequate timescales for completion. To be incorporated into the annual data audit	January 2018	
		Right to be forgotten	Fund will need a process for managing and actioning these requests as well as determined reasons why deletion may not be appropriate.	January 2018	
		Data Portability	Fund needs a process for actioning these requests and for ensuring data is held in a portable form.	January 2018	

Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status
Consent	Implied consent permitted	Express consent must be given. Must be clear and unambiguous for each purpose. We must keep records of consent received (so we can demonstrate we have received it). Data subjects must be able to withdraw consent at any time and as easily as it was to give it.	Review forms and documents to ensure they provide information of all uses of information (including AVC). Ensure they provide for consent over and above "tick box".	ASAP	
Subject Access Requests	Provides for a £10 admin fee and allows 40 days to respond	Removes £10 charge (which may increase requests) reduces time period to respond to one month	Need to review the processes with WCC IG team to ensure the timetable is met, may require additional resource due to time reduction	ASAP to encourage good practice	
Data Retention Periods	For as long as required	Need to be clearly defined	Review processes to confirm timescales for holding data for each process Draft and publish data retention policy.	ASAP	Discussions ongoing with software provider to have this facility built in to the Fund's software.

Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status
Data Breaches	To notify WCC IG team who make determination on whether to report	As a processor the duty will be on us to report with greater reporting requirements, including notifying member	Training to be delivered to staff on new regulations and duties to protect data. Greater scrutiny of staff actions in this area. Tighter policies on reporting.	Training to be delivered in January 2017 and updated in June 2017 Policies to be written and implemented by January 2018.	
International Members	Covered the same as DPA in EU countries	Now applies to companies operating outside the EU who have data subjects within the EU	Particularly significant in relation to Brexit and our international members. May need to consider that there will be different requirements on handling their data.	Need to wait for further regulations/guidance as unclear at this time.	

Area for Action	Current Regulation	New Regulation	Action required to ensure adherence	Timescale	Status

Policies to be drafted/incorporated	Policies to be reviewed
• Data Retention policy • Data Portability • Transfer of data • Consent • Right to rectification • Right to be forgotten • Process maps to show use of data for all fund processes • International members • Privacy impact assessments for all fund processes • Annual data cleanse/review • Transparency (how we use your data) policy • Children's transparency policy	• Subject access requests • Data sharing agreement • Third party contracts • Reporting Data breaches • Privacy notices