SYPA Record of Breaches

Year	Ref	Date Identified	Type of Breach (e.g. personal data, contributions, criminal activity, etc)	Description	Action Taken in Response to Breach	Possible Impact (Red/Amber/ Green)	Date Reported to Local Pension Board or Authority	Reported to Pensions Regulator or other statutory body (e.g. ICO)?	Reported to Data Protection Officer?	Details of any follow up actions taken/required or wider implications	Breach Open/Closed
2021/22	56	08/10/21	Personal Data	Single listing of AVC Premiums from AVC Provider was made available on member record on *MyPension* portal. Details of other members had been blanked out but were still visible.	Apologised to member for individual error. All other member records did not display personal details.	Green	27/01/2022 (LPB)	NO	NO	Indexing updated on system to make it clear document is visible to member. See also Ref 58.	Open pending any Board comments
2021/22	57	19/11/21	Personal Data	Medical report issued to incorrect contacts at employer (issued to decision maker and former line manager rather than OH team)	Recipients confirmed they have deleted report and it was re-issued to correct contact.	Green	27/01/2022 (LPB)	NO	NO	New member of staff provided with additional procedural training.	Open pending any Board comments
2021/22	58	29/11/21	Personal Data	Single listing of AVC Premiums from AVC Provider was made available on member record on *MyPension* portal. Details of other members had been blanked out but were still visible. Same error as Ref 56 but further action taken.	Apologies to member and confirmed document removed.	Green	27/01/2022 (LPB)	NO	NO	Team identified Ref 56 was still subject to individual error so indexing changed globally to completely remove visbility on *MyPension* .	Open pending any Board comments

Year	Ref	Date Identified	Description of Cybersecurity Incident	Action Taken in Response to Incident	Date Reported to Local Pension Board or Authority	Reported to Pensions Regulator or other statutory body (e.g. ICO)?	Reported to Data Protection Officer?	Details of any follow up actions taken/required or wider implications	Incident Open/Closed
2021/22	CS13	02/12/21	Phishing email received by member of the Engagement team purporting to be from an employer contact.	All users informed of phishing email. The links included in the email were not followed and have been blocked.	27/01/2022 (LPB)	NO	NO	NCSC cybersecurity elearning course recently undertaken by all staff. Further phishing email testing is planned as part of IT work programme to check users remain vigilant.	Closed
2021/22	CS14	05/12/21	Phishing email received by Head of Pensions Admin stating domains had expired.	The sender was blocked and URLs also blocked. Appears to be hacked farming equipment site! Checked and no other recipients received email.	27/01/2022 (LPB)	NO	NO	As above.	Closed