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
2020/21		31/03/22	Compliance	Prudential have confirmed they have failed to meet 12 month deadline for issuing AVC statements.	Prudential have already notified TPR but SYPA also issuing report for completeness.	Red	28/04/2022 (LPB)	YES	NO	Wider review of AVC provision being undertaken by external provider.	Open pending any Board comments
2020/21			Compliance	Pension Saving Statements were issued late for 2020/2021	See separate report at 28/4/22 Board meeting.	Amber	28/04/2022 (LPB)	?	NO	See separate report at 28/4/22 Board meeting.	Open pending any Board comments
2022/23	59	08/04/22	Personal Data	Set of data queries on MDC file were sent encrypted to wrong Council payroll department.	Recipient requested to delete data and supervisory discussion with member of staff.	Green	28/04/2022 (LPB)	NO	NO	Further development required by Civica (by Sept 22) and then routine queries will be sent via portal instead.	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	CS15	04/03/22	Phishing email sent to two members of SYPA staff containing a link to a fake Microsoft login page.	Emails were blocked by Mimecast as Spam and not released. The sender was blocked and URLs also blocked.	28/04/2022 (LPB)	NO	NO	NCSC cybersecurity elearning course previously undertaken by all staff. Further phishing email testing is planned as part of IT work programme to check users remain vigilant.	Closed