DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: The Chief Constable of South Yorkshire Police (SYP)

OF: Carbrook House
Carbrook Hall Road
Sheffield
S9 2EG

1.1 The Information Commissioner (the Commissioner) issues a reprimand to South Yorkshire Police in accordance with Schedule 13(2)(c) of the Data Protection Act 2018 (DPA 2018) in respect of certain infringements of the DPA 2018.

The reprimand

1.2 The Commissioner has decided to issue a reprimand to SYP in respect of the following infringements of the DPA 2018:

- **Section 34 (3) Part 3 of the DPA18** 'compliance' which states the controller, in relation to personal data is responsible for, and must be able to demonstrate, compliance.
- **Section 40 Part 3 of the DPA18** 'the sixth data protection principle' which states that personal data that is processed for any law enforcement purposes must be so processed in a manner that ensures appropriate security of personal data using appropriate technical or organisational measures.

1.3 The reasons for the Commissioner's findings are set out below.

1.4 SYP is the territorial police force responsible for policing in South Yorkshire. The force was formed in 1974 as a merger of the previous Sheffield and Rotherham Constabulary along with part of the West Yorkshire Constabulary area (which Barnsley Borough Police and Doncaster Borough Police had merged into on 1 October 1968). SYP's jurisdictions cover 1,554 square kilometres and a population of 1.28 million.

1.5 SYP's fundamental purpose is law enforcement and as such it routinely captures and processes personal data of individuals whilst carrying out those duties. SYP determines the purpose and means of that processing; therefore, SYP is the data controller responsible for these infringements.

1.6 As part of SYP's duties, SYP routinely use Body Worn Video (BWV) as an overt method to capture both video and oral evidence when attending all types of incidents. BWV equipment and software is supplied to SYP by a third party. At the time of the contravention, that third party was responsible for Digital Evidence Management (DEMS), a software solution that allows police departments to manage all digital evidence in one secure central hub. The use of BWV is intended to increase public reassurance, capture best evidence, modify behaviour, deter criminal and anti-social behaviours and to increase transparency & build public trust. Other benefits include a reduction on reliance on victims' evidence due to BWV footage being impartial and accurate.

1.7 BWV footage may contain images or audio of individuals which may disclose or infer an individual's personal data, some of which could be considered to be special category data. For example, an individual's, health data, criminal convictions or biometric data.

1.8 Once captured by SYP Officers, the BWV footage is downloaded to a docking point at the end of a shift and transferred to DEMS, which is then transferred to a secure storage repository. At the time of the contravention, SYP used and was responsible for a storage repository called the Storage Grid.

1.9 Following an upgrade of DEMS in May 2023, the system was struggling to process data from the Storage Grid, so a workaround was put in place to store it locally. Therefore, at the time of the deletion, the primary storage of BMV footage was by local disk on the application server, although the data was still available on the Storage Grid for viewing by the users.

1.10 On 26 July 2023, the third party was carrying out data transfer activities in regard to the movement of data from the local drives onto the Storage Grid storage location as part of the overall support arrangements provided as a supplier of the DEMS application.

1.11 On 7 August 2023 an IT manager at SYP identified that the file storage on the Storage Grid was very low which indicated files were

missing from the Storage Grid. On further investigation it was found that 96,174 pieces of original BWV footage had been erroneously deleted from The Storage Grid.

1.12 On 11 September 2023 SYP conducted a digital forensic investigation, the results of which found that there had been a mass deletion of data (BWV footage) which had taken place on 26 July 2023.

1.13 SYP has not been able to provide a definitive explanation as to how the deletion occurred, however, SYP has explained that it believes the data (BWV footage) was deleted from the Storage Grid in error.

1.14 SYP further explained that when the mass deletion took place on 26 July 2023, 96,174 pieces of BWV footage were permanently removed from the Storage Grid.

1.15 However, prior to this, as part of the process for retaining evidential material, 95,033 pieces of that BWV footage had previously been copied from the Storage Grid on to a new system, named the Digital Asset Management System (DAMS). This is a software solution that manages digital evidence. Some of the copies of BWV footage held on DAMS were full copies of footage, some were snippets and some were duplicated. SYP are unable to confirm the exact numbers of footage that has been deleted without copies being made.

1.16 When BWV footage was copied over to the DAMS system, SYP directed that all files that were copied did not have to be individually named and should be recorded as 'generic'. This was because of the small numbers of BWV files that were required to be copied into each criminal investigation, and SYP did not consider it necessary to label the footage more clearly, for example by using specific file names or other identifiable means of tagging the data. Therefore, SYP are unable to accurately compare data sets to determine an accurate volume of original BWV footage that has been permanently deleted and lost.

1.17 The ICO's investigation found that despite a contract being in place between SYP and the third party, documenting each parties' responsibilities, it did not provide any granular detail to specify how this processing was to be carried out. SYP routinely provided role specific remote access to the third party; however, SYP failed to have any

effective oversight or monitor how work was being carried out by the third party.

1.18 Following the loss of BWV footage when transferring the data from the local temporary storage to the Storage Grid, SYP ran a backup of the files, which resulted in the recovery of BWV files up to 21 July 2020. Despite several attempts to restore the data, SYP has failed to recover any of the BWV footage that had been transferred and uploaded to the Storage Grid since 21 July 2020. This is due to unresolved issues with the backup solution, which were identified in 2019. At that time, the IT Server manager reported a general risk in relation to the backup capacity but failed to provide specific detail that would have explained that the backup capacity had failed. Due to the full extent of these problems not being reported to Senior Leadership, no remedial action was taken to rectify the problems with the backup solution and only in August 2023 was the extent of the issue realised.

1.19 The data loss included 126 criminal cases, however, only three of the criminal cases were affected by the data loss. SYP have advised however, that of these three criminal cases it is very unlikely that two of these cases would have proceeded to the first court hearing due to other factors. The third case may have progressed if BWV had been available, however there was no additional independent evidence to prove the offence, therefore progression to prosecution stage was already uncertain.

1.20 Furthermore, SYP has been unable to provide BWV footage for nine civil claims and one Judicial Review and cannot respond to four SARs.

1.21 **In order to comply with Section 34 (3) Part 3 of the DPA18** 'compliance', SYP should have implemented appropriate technical and organisation measures to ensure it can demonstrate that it complies with the principles set out in Part 3 of the DPA18.

1.22 The ICO investigation found that SYP failed to follow its own policies in relation to the security of its information systems. SYP delayed formalising an IT Backup Policy which would have provided details on how backups should be completed. The investigation found that due to poor record keeping SYP are unable to confirm how many original pieces of BVW footage has been permanently deleted. Therefore, SYP cannot demonstrate it has complied with its data protection obligations.

1.23 **In order to comply with Section 40 Part 3 of the DPA18** 'the sixth data protection principle' SYP should have ensured that as the controller, it had appropriate technical and organisational measures in place to prevent the accidental loss, destruction, or damage of personal data.

1.24 Prior to the introduction of the use of BWV, despite SYP completing a DPIA, the ICO investigation found that no specific security risk was identified in relation to the transfer, loss or unavailability of BWV footage. Therefore, SYP failed to ensure it had adequate measures in place to mitigate against any loss of BWV footage.

1.25 SYP could not provide any documentary evidence to show a risk assessment had been carried out in relation to third party access to SYP information systems and in particular to establish specific controls.

1.26 SYP routinely provided unchecked role specific access to the third party to DEMS and the third party was able to determine which method it used when undertaking its duties. [redacted]

Remedial steps taken by SYP

1.27 The Commissioner has also considered and welcomes the remedial steps taken by SYP in the light of this incident. In particular.

- Reviewing the potential impact of the loss of BWV footage prior to cases being referred to the Crown Prosecution Service (CPS) and risk assessing each case against how the unavailability of the BWV footage would affect the case and /or victim. As part of the criteria SYP considered the probable content of the footage, what other evidence is available, and the impact on the case.

- Attempting to restore the BWV footage.

- Creating a plan which included informing those affected individuals of the loss of BWV which took place on a case-by-case basis.

- Releasing a press release to inform data subjects of the loss of BWV footage.

- Shadowing third parties when accessing DEMS.

Decision to issue a reprimand

1.28 Taking into account all the circumstances of this case, including the remedial steps, the Commissioner has decided to issue a reprimand to SYP in relation to the infringements of sections of the DPA 2018 set out above.

SYP were invited to provide representations. SYP provided representations on 27 May 2025.

Further Action Recommended

1.29 The Commissioner has set out below certain recommendations which may assist SYP in rectifying the infringements outlined in this reprimand and ensuring SYP future compliance with the DPA 2018. Please note that these recommendations do not form part of the reprimand and are not legally binding directions. As such, any decision by SYP to follow these recommendations is voluntary and a commercial decision for SYP For the avoidance of doubt, SYP is of course required to comply with its obligations under the law.

1.30 If in the future the ICO has grounds to suspect that SYP is not complying with data protection law, any failure by SYP to rectify the infringements set out in this reprimand (which could be done by following the Commissioner's recommendations or taking alternative appropriate steps) may be taken into account as an aggravating factor in deciding whether to take enforcement action - see page 11 of the Regulatory Action Policy Regulatory Action Policy (ico.org.uk) and section 155(3)(e) DPA 2018.

1.31 The Commissioner recommends that SYP should consider taking certain steps to improve its compliance with DPA 2018. With particular reference to section 34 (3) and 40 of the DPA 2018, the following steps are recommended:

1. Continue to provide any necessary support to help mitigate any potential detriment caused to the affected data subjects where appropriate.

2. Continue to shadow third parties as appropriate when accessing SYP's information systems.

3. SYP should ensure that there is an adequate storage backup solution in place and ensure that it has an effective process in place to restore any lost BWV footage.

4. SYP should define roles and responsibilities for third parties and in particular when processing personal data held on its information systems.

5. When completing a review of the DPIA relating to DEMS, SYP should ensure all risks are identified, and in particular any risks regarding the potential loss of BWV footage and adequate backup solutions. The review should also ensure that SYP takes steps to mitigate against such risk.

6. SYP should complete a risk assessment to determine security implications and control requirements prior to permitting third parties' access to SYP's information systems.

7. SYP should ensure all records are marked in a clear and concise way.

6 June 2025