DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Chief Constable West Midlands Police

OF: PO Box 52, Lloyd House, Colmore Circus Queensway, Birmingham, B4 6NQ

1.1 The Information Commissioner (the Commissioner) issues a reprimand to Chief Constable West Midlands Police (WMP) 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 WMP in respect of the following infringements of the DPA 2018:

- Section 34(3) which states "The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter."

- Section 38(1) which states "The fourth data protection principle is that - (a)personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and (b)every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay."

- Section 38(3) which states "In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as - (a)persons suspected of having committed or being about to commit a criminal offence; (b)persons convicted of a criminal offence; (c)persons who are or may be victims of a criminal offence; (d)witnesses or other persons with information about offences."

- Section 40 which states "The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage)."

- Section 57(1) which states "Each controller must implement appropriate technical and organisational measures which are designed - (a)to implement the data protection principles in an effective manner, and (b)to integrate into the processing itself the safeguards necessary for that purpose."

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

1.4 This case relates to two individuals with the same name and date of birth, whose personal data is processed by WMP, which is a large regional police force. Since as early as January 2020, WMP incorrectly linked and merged the records of these two individuals with similar personal data on multiple occasions. This led to inaccurate personal data being processed on WMP's systems and resulted in a number of incidents, for example: where WMP officers attended the wrong individual's address when attempting to locate the other individual for which they had serious safeguarding concerns relating to domestic violence; and attending the wrong individual's child's school when attempting to locate the other individual. These incidents included events where personal data was either actually or potentially inappropriately disclosed.

Section 34(3)

1.5 WMP failed to demonstrate that they have ensured the accuracy and security of personal data relating to the two individuals in this case. WMP do not hold adequate records of the incidents relating to the accuracy and security of these individuals' personal data. The Commissioner found that this had a negative impact on WMP's ability to monitor and rectify non-compliance with the data protection principles.

Section 38(1)

1.6 On numerous occasions throughout 2020, 2021 and 2022, information relating to one individual was incorrectly linked to the other individual's record. Due to inadequacies in WMP's record keeping and incident management, the number of times incorrect linking occurred and the durations for which such inaccuracies were present on WMP's systems are unknown. The full impact of the processing of inaccurate personal data is also not known to WMP. The true number of times officers attended the incorrect individual's address (or child's school) is unknown, although there are at least four dates where there are suggestions this may have occurred.

1.7 WMP are unable to demonstrate that inaccurate personal data was rectified without delay. Where remedial actions were taken by WMP, such

as adding a note to the relevant system warning officers of the two individuals with similar personal data, such actions failed to prevent the inaccurate linking of records recurring.

1.8 Following the launch of the "[redacted]" system in April 2021, and again in January 2022 following the launch of the "[redacted]" system, the records of the two individuals were incorrectly merged. WMP unmerged the records on the [redacted] system, however are unable to unmerge the records on the [redacted] system, resulting in the ongoing processing of inaccurate personal data relating to the two individuals.

Section 38(3)

1.9 In this case, one of the individuals is known to WMP as the victim of a crime whereas the other individual has been known to WMP as both a suspect and a victim. Due to the incorrect linking and merging of the two individuals' records, WMP have not made a clear distinction, as far as possible, between the personal data of victims and suspects of crime, as is required.

Section 40

1.10 On 12 July 2022, WMP sent a letter to one individual that was intended for the other, disclosing that they had been a victim of an assault. At this time, the recipient was aware of the data accuracy issue on WMP's systems and that this letter related to an individual who shares their name and date of birth and lives in the local area.

1.11 In addition to the above security incident, WMP have failed to demonstrate that they have kept personal data secure in relation to the other incidents affecting these two individuals. Due to the lack of appropriate records of these incidents, WMP do not know whether personal data was disclosed, including information concerning criminal offences. WMP have assessed that, on the balance of probabilities, the security of information relating to criminal offences was affected by the relevant incidents.

Section 57(1)

1.12 The Commissioner found that WMP failed to implement appropriate technical and organisational measures to implement the data protection principles in an effective manner.

1.13 As outlined above, WMP consider one merging of the individuals' records to have been the result of the implementation of the [redacted] system. The testing and risk assessment of the [redacted] system carried out by WMP failed to prevent the inaccurate merging of records of the two

individuals or identify the need for a manual editing tool, enabling such records to be separated on the system. Since the need for a manual editing tool has been identified, the development of this tool has not progressed in a timely manner, meaning WMP have been unable to rectify inaccurate personal data without delay.

1.14 WMP have not demonstrated that they provided employees with clear policies, procedures and training relating to use of the [redacted] system. Regarding mandatory data protection training, the Commissioner notes that WMP reported difficulty in providing an accurate figure of the number of employees who completed data protection training within the last two years, but estimate this is between 30 and 35%. Additionally, due to inadequate records of the incidents relevant to this case, WMP are unable to identify the employees involved in all but one of the incidents, meaning they are unable to direct those employees to complete refresher training following their involvement in an incident, as is required by WMP policy.

1.15 The Commissioner also found that WMP did not do enough to make employees aware of their responsibility to report inaccurate personal data identified on WMP's systems to the Information Management team.

Mitigating factors

1.16 In the course of our investigation we have noted that WMP provided one of the affected individuals with compensation and a letter to help them address similar data accuracy issues occurring with other organisations.

Remedial steps taken by WMP

1.17 The Commissioner has also considered and welcomes the remedial steps taken by WMP in the light of this incident. In particular, WMP produced a new Data Quality Policy and carried out a "Think before you link" communications campaign, which reminded employees to ensure links between connected individuals are accurate.

1.18 It is noted that WMP repeatedly manually unlinked the records of the two individuals and added notes to the relevant systems regarding the similar personal data. However, these remedial actions were ineffective in preventing future incidents and ensuring compliance with the data protection principles.

Decision to issue a reprimand

1.19 Taking into account all the circumstances of this case, including the mitigating factors and remedial steps, the Commissioner has decided to

issue a reprimand to WMP in relation to the infringements of sections of the DPA 2018 set out above.

1.20 WMP were invited to provide representations, which were submitted to the ICO on 16 January 2024 and are summarised below.

Further Action Recommended

1.21 The Commissioner has set out below certain recommendations which may assist WMP in rectifying the infringements outlined in this reprimand and ensuring WMP's 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 WMP to follow these recommendations is voluntary and a commercial decision for WMP. For the avoidance of doubt, WMP is of course required to comply with its obligations under the law.

1.22 If in the future the ICO has grounds to suspect that WMP is not complying with data protection law, any failure by WMP 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 and section 155(3)(e) DPA 2018.

1.23 The Commissioner recommends that WMP should take certain steps to ensure its compliance with the DPA 2018. The following steps are recommended:

1. In order to ensure compliance with section 34(3) WMP should maintain relevant records of its processing activities and take steps to improve governance measures, including considering guidance on the ICO website: Accountability and governance

2. In order to ensure compliance with sections 38(1) and 38(3) WMP should take appropriate action to distinguish the records of the two individuals and prevent further inaccurate linking and merging of records containing personal data. This should include completing the technical changes needed to unmerge the records on the [redacted] system in a timely manner.

3. In order to ensure compliance with section 40 WMP should ensure learnings from security incidents are shared across the organisation and that employees are reminded of relevant security policies.

4. In order to ensure compliance with section 57(1) WMP should ensure employees attend mandatory data protection training in line with

WMP policies, including implementing an appropriate action plan to improve completion rates of refresher data protection training. WMP should also consider implementing clear policies, procedures and training that is specific to the use of the [redacted] system.

1.24 On 16 January 2024, WMP submitted representations to the ICO advising the Commissioner of progress that has been made in respect of the above recommendations:

- The Commissioner recognises that WMP have made improvements in relation to recommendation 1 and implemented new accountability and governance measures.

- In respect of above recommendations 2 and 3, the Commissioner considers that these recommended steps have been completed.

- In respect of the relevant trainings in place, during representations WMP advised that training is provided prior to employees being granted access to new systems, including the [redacted] and [redacted] systems. The Commissioner also acknowledges that WMP has made progress regarding recommendation 4, including reviewing relevant trainings and developing an action plan to improve completion rates of refresher data protection training.

1.25 We invite WMP to provide a further progress update on the above recommendations in six months of the date of this reprimand.