Police Superintendents' Association

26.07.2018

Project Cadmium

Working Time Regulation Project

Data Management Protocol

Commissioned by Chief Superintendent Dan Murphy

NATIONAL GENERAL SECRETARY – POLICE SUPERINTENDENTS ASSOCIATION

DATA COLLECTION PLAN

PROJECT BACKGROUND

There has been increased demand placed upon policing by reductions in the number of police officers. The service is relying on fewer officers working longer hours to meet that demand. Since 2010 the number of Superintending ranks across England and Wales has dropped by approximately 25%.

Members of The Police Superintendents' Association (PSA) have been significantly affected by the resulting increase in with their responsibilities and the associated range and complexity of their duties. Long working hours have been undermining the wellbeing of our members for some time.

The PSA has been trying to resolve this situation since 2010. It has commissioned various independent surveys on pay, resilience, morale and motivation, and used the results as a basis for constructive engagement.

These surveys have consistently shown that superintendents are:-

- Working longer hours
- Working on their rest days
- Working on their annual leave days
- Unable to take all their annual leave
- Unable to take all their rest days
- Undertaking more periods on-call
- Undertaking on-call duties on their annual leave and rest days

The latest Resilience Survey attached below (Joint PSA, SANI and ASPS Resilience survey conducted late 2016) confirmed that 78% of Superintendents are working more than 50 hours per week, exceeding the 48-hour limit imposed by the Working Time Regulations 1998 ("WTR"). Most are working rest days and annual leave days, and spending more time on call. More than half of the respondents reported symptoms of anxiety and more than a quarter symptoms of depression. This is having a negative impact on their wellbeing and may be adversely affecting their performance at work.

PROJECT SCOPE

The PSA wants better to understand the demands placed upon its members. This project concerns gathering information in order to produce an accurate picture of hours worked by members and the reasons why many are working long hours.

The parameters of the project are based on the Working Time Regulations identified below:

Regulation 4	Regulation 10	Regulation 11	Regulation 12	Regulation 6	Regulation 24
48 hr working week.	Daily rest period of 11 consecutive hours.	Weekly rest period of 24 hours. Must be consecutive with daily rest period in most cases. Two rest days may be taken every fourteen days instead.	Daily rest break of at least 20 minutes after six hours work.	Night worker must not work more than average of 8 hours in 24.	Compensatory rest where worker required to work through rest period or break, depending on circumstances.

ETHICS & LEGAL COMPLIANCE

This project will comply with the following principles:

1. Reliance on consent that is freely given and fully informed
2. Openness and integrity
3. Protection of the rights to privacy of individuals

Consent

The project will collect personal data only with the express consent of the participant. This permission will be sought by use of an electronic form which provides the following information about the project:

- PowerPoint presentation
- Strategic objective and success measures
- Frequently asked questions
- Participants' obligations
- Participant's right to withdraw consent at any time
- Destruction of personal data where consent is withdrawn.

Openness and Integrity

The Cadmium project initiation document clearly outlines the intent of the project and its scope. The collation of data will be for that purpose. In the unlikely event that the PSA wishes to us personal data collected for any other purpose, further consent will be obtained.

Participants will be provided with access to the outcomes of the research in which they have participated and debriefed if they consider it necessary after they have provided data.

By participating in the project members will learn whether their own working patterns comply with the WTR and provide valuable information to the PSA, enabling it to assess national compliance with the WTR and the impact on health and wellbeing of non compliance.

Protection of rights to privacy

No personal data will be shared externally, without the express permission of the participant. Information provided to the National Police Chiefs' Council will be anonymised.

The PSA will take reasonable steps to ensure that the information gathering exercise complies with the General Data Protection Regulation. In the event of any suspected breach of the Regulation by the PSA which adversely impacts on a participant's right to privacy, each participant agrees not to take any action relating to the breach without first attempting to resolve the situation with the PSA National Executive Committee.

DATA COLLECTION & SECURE STORAGE

Data will be collected using a bespoke data collection template designed utilising Microsoft Excel software. Project participants will enter data via this software either using Microsoft Excel online or through the Microsoft Excel software as a desktop version. The data submitted will be monitored and reviewed remotely to assist with the delivery of the project objectives by the PSA project management support.

The Police Superintendents' Association uses Microsoft Office 365 Business. The data provided will be stored in the Microsoft OneDrive account operated by the Police Superintendents' Association. Access to this data is restricted and the PSA remain the sole owner: retaining the rights, title, and interest in the data. Microsoft clearly outline that the data stored in Office 365 is "your data."

Albeit the data to be collected is not considered moderately or highly sensitive, it will be security and privacy protected given there are appropriate levels of defence in depth when using the Microsoft OneDrive system.

Some of the Microsoft OneDrive systems security and compliance features are outlined below to illustrate that data security has been thoroughly considered:

Physical security

- 24-hour monitoring of datacentres.
- Multi-factor authentication, including biometric scanning for datacentre access.
- Internal datacentre network is segregated from the external network.
- Role separation renders location of specific customer data unintelligible to the personnel that have physical access.
- Faulty drives and hardware are demagnetised and destroyed.

Logical security

- Lockbox processes for a strictly supervised escalation process greatly limit human access to your data.

- Servers run only processes that are whitelisted, minimising risk from malicious code.
- Dedicated threat management teams proactively anticipate, prevent, and mitigate malicious access.
- Port scanning, perimeter vulnerability scanning, and intrusion detection prevent or detect any malicious access.

Data security

- Encryption at rest protects your data on our servers.
- Encryption in transit with SSL/TLS protects your data when it's transmitted between you and Microsoft.
- Threat management, security monitoring, and file/data integrity prevent or detect any tampering of data.
- Exchange Online Protection provides advanced security and reliability against spam and malware to help protect your information and access to email.

User controls

- Office 365 Message Encryption allows users to send encrypted email to anyone, whatever email service recipients may use.
- Data loss prevention can be combined with Rights Management and Office 365 Message Encryption to give greater controls to your admins to apply appropriate policies to protect sensitive data.
- S/MIME provides message security with certificate-based email access.
- Azure Rights Management prevents file-level access without the right user credentials.

The data will be collected over a 21-week period.

A frequently asked questions paper will be made available to participants so as to ensure the data they provide is accurate and relevant.

Each participant will be provided with their own data template link on which to enter their data. This link is personal to the participant and will be seen by nobody else other than PSA representatives. No other participant will be able to view other participant's data.

The data collated is set out within the data collection template and which includes:

- Participant's name and force
- Period designation
- At Workplace working time
- Agile working time

- On call working time
- Recording of activities for other work periods
- Duty time periods
- Has the duty been recorded on the force system?
- On call duty type
- On call time periods
- Uninterrupted breaks and associated time periods
- Participant's personal notes
- Various time calculation totals

DATA ANALYSIS & REVIEW

Analysis and review of participant data will take place both during the project and at its conclusion. This data will be analysed at an individual and branch level.

Only non-personalised data will be available to the National Police Chiefs Council.

We will provide anonymised data to forces and work with them to develop a framework for understanding the Superintending rank resource requirement.

DATA DESTRUCTION

At the end of the project, the PSA NEC will determine how long the personal data needs to be retained. Much will depend on whether the project's objectives have been achieved. Participants will be notified of the proposed destruction date by no later than 31 March 2019.