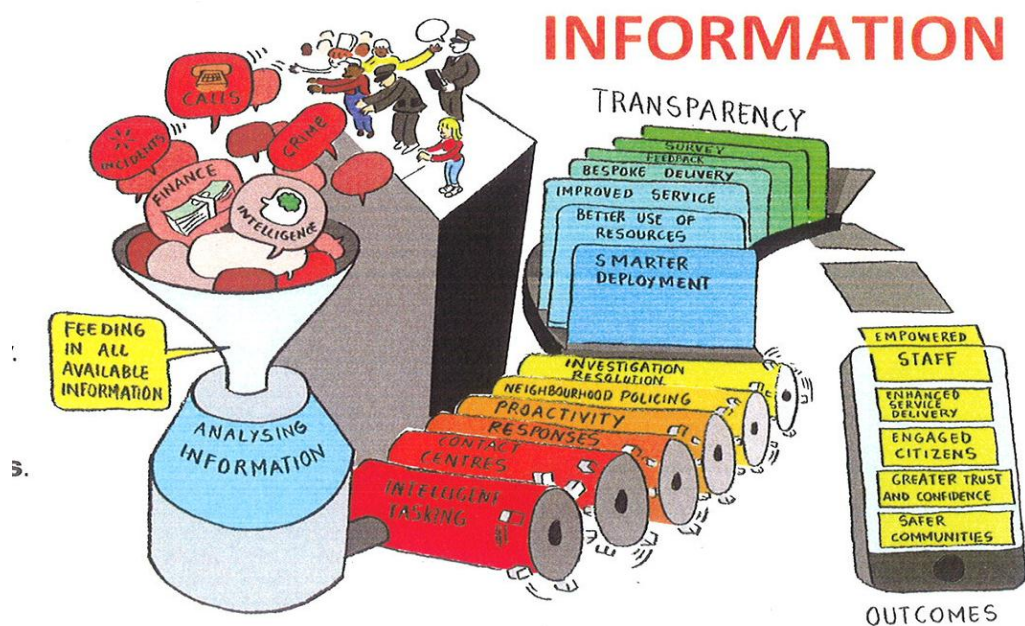


Information Management Strategy



Information Management Strategy

Introduction

The force has a number of information related policies and documents that combine to describe WMP's approach to information management.

Information Management

1. The force's risk appetite statement provides the context in which risk will be managed. It is reviewed annually by the Strategic Information Management Board (SIMB).
2. The information management policy (inf/01) lays out who is responsible for information within force and this is expanded on in the Information Asset register which also records which business areas hold information. This policy includes information on our approach to audit.
3. The data protection policy explains why the force collects data and the safeguards that are applied to it. The information security policy (inf/06) gives more detail on the security of information, controls applied and related training requirements.
4. The information risk policy (inf/18) sets out the processes for assessing risks associated with new projects and other change. It includes details of the key roles in information assurance/management.

5. The compliance, audit and assurance policy covers the force's approach to complying with national and local security policy and procedures and gives further detail on the roles involved in these processes.

Governance

The strategy and associated policies are owned by Senior Information Risk Owner (SIRO) who discharges this duty through the SIMB. The monthly information assurance workgroup (IAWG) provides tactical support to the SIMB and reviews policy on an annual basis.