Item 6 Appendix C

DORSET & WILTSHIRE FIRE AND RESCUE AUTHORITY
Information Management Policy

The Dorset & Wiltshire Fire and Rescue Authority (DWFRA) is the combined fire and rescue authority for its area, as defined within sections 1 and 2 of the Fire and Rescue Services Act 2004. This document contains the Authority's policy on information management. It is supported by a set of procedures.

Information is an important organisational asset and we need to make sure we properly and efficiently manage and protect the information we hold. We constantly work on making sure our information is complete, accurate, relevant, accessible, and timely. As well as ensuring legal compliance, the Authority requires a high standard of governance to support open and transparent decision-making.

In line with our vision, we strive to continue to be a trusted partner. We share and receive information responsibly by following good practices and, where appropriate, secure recognition of this through externally accredited standards.

We have established effective information management systems embedded and maintained throughout the organisation. These systems directly support our strategic aims/vision and the need to ensure legal compliance against a range of statutory requirements. We take advantage of cost effective technology to make sure appropriate and secure solutions are in place to support the management of the information we hold.

This policy and the supporting procedures are:

- the responsibility of a nominated Senior Information Risk Owner (SIRO) within our Senior Leadership Team (SLT)
- reviewed annually by senior management and scrutinised by Members as part of the Statement of Assurance. This Statement and our assurance framework are publically available to promote confidence in the Authority and its Service.

Why is this policy needed?

As a Fire and Rescue Authority, we need to:

- demonstrate and make sure high standards of governance and management are in place throughout the organisation
- comply with the Data Protection Act 1998, Freedom of Information Act 2000, Environmental Information Regulations 2004 and the Regulation of Investigatory Powers Act 2000

- make sure the public has faith in our information and how we manage it
- guarantee decision making is supported by efficient and legally compliant data and information management
- ensure the right people have the right information at the right time
- minimise the risk of unauthorised people having access to our information
- make use of technology to provide efficient, effective and secure information management
- manage significant financial liabilities and risks.

How we will meet the above requirements?

In order to reach our objective(s), we make sure our staff have the knowledge, skills and capacity to successfully deliver this policy through the following procedures and/ or frameworks:

Managing personal information – We provide procedures on the processing, storage, security, retention and disclosure of our personal information and effective electronic systems that supports this.

Accessing information – We encourage and demonstrate openness and transparency of our information and provide measures for releasing appropriate information in line with our legal duties.

Staff awareness and engagement – We make sure staff awareness and training occurs at induction, and while in role. We review this through various methods, such as, personal appraisals.

Policy Framework – We target our policies and procedures to the right people; use Plain English and consider our legal requirements in a consistent way by using a standardised format. We make sure policies and procedures are up-to-date and readily available to all staff.

Data sharing – we share information securely with our partners, improving prevention and response activity, and ensure data sharing is appropriately managed.

Information security – We use the ISO 27001 Code of Practice for Information Security Management as our framework to safeguard the confidentiality, integrity and availability of our information.

ICT – We guarantee all staff who access our systems are aware of their responsibilities for acceptable use.

Success of the Policy – How is this Policy assured?

This policy document was the subject of external verification during its development.

In order to monitor and continue to meet the above requirements:

- the results of an assurance process focusing on legal compliance will be provided to the Fire and Rescue Authority in support of the Statement of Assurance
- we will conduct and manage an annual ICT Health Check with corrective action plan

- we manage information risk against the Information Management Framework and regularly monitor this during the Information Governance group meetings
- we work with external inspectors and conduct internal audits regularly in accordance with the prioritised audit plan
- we consistently review risk assessments to make sure latest threats and exposures are appropriately considered
- we put in place an incident handling process that includes appropriate management review to make sure changes to policies and procedures are identified and implemented.

Review Date

This policy will be reviewed at least every three years or will be brought back to Members if requirements change.