Appendix 7
to Item No: B1

Kent and Medway Fire and Rescue Authority

Performance and Data Strategy 2018-22

Contents

Introduction

The Authority is a high performing local authority, and strives to be open and accountable to the customers it serves both internally and externally. This Strategy, which is one of a set which underpin the Customer and Corporate Plan, sets out how we will deliver even greater transparency, in a safe and secure data environment. It also sets out how good quality data drives evidence-based decision-making, which in itself can deliver value for money to the taxpayers of Kent.

It supports all the actions within the Customer and Corporate Plan. With good data and systems:

- the value of our interventions can be evaluated, lessons can be learned and improvement actions can be developed and implemented;
- Partnership working can happen effectively by data-sharing between practitioners;
- Public trust and confidence can be maintained through open performance assessment, and not being subject to security breaches.

This Strategy also supports the functioning of all the other supporting Strategies. Where work is specific to this Strategy, it is shown in the action plan at the end, which has indicative timescales and a responsible officer.

Deviations from this Strategy will be agreed at CMB, and an annual assessment of progress will be provided to Members.

This Strategy does not cover the recording of skills through training, nor appraisal training. Approaches to these issues are dealt with in other Strategies within this set.

Governance

We have designated a member of Corporate Management Board as the Authority's Senior Information Risk Officer, and this is embedded within their job description. Issues relating to data, such as amendments to policy, are reported to Corporate Management Board for approval before being approved by Members. We have an agreed publication and retention scheme, last approved by Members on 18 October 2017.

We have robust processes for dealing with requests for data or information, and perform well in responding to these requests within 20 working days (where appropriate). Performance is reported to Members as part of the annual feedback report, and also as part of the governance assurance process.

The Service has a robust process for reporting data security incidents which is integrated into business continuity arrangements.

We have not set up an information governance group. Whilst it is recognised that this would be best practice, it is not felt that it is warranted at the current time. The reasons for this decision is that there is no evidence of significant data breaches arising from the Service's network, nor are the volume of data requests such that significant business could be given to such a group to transact. Instead, information governance is considered by Corporate Management Board.

Every aspect of our support services is also scrutinised as we seek to learn. There are good practice and regulatory frameworks in place for every aspect of support services. Everyone that works for us in support services is encouraged to maintain their professional skills as a mechanism to ensure quality. In certain professions this can include membership of professional bodies for which continuous professional development records have to be maintained.

Scrutiny is provided through feedback and debate, and we use that to change many aspects of what we do. Members provide scrutiny through Authority meetings of all of the Service's work. We also have external and internal audit bodies who look in detail at many aspects of our processes and practice. We use the LEAN (a way of looking at maximising customer service and simplifying the customer journey through our systems by reduction of waste, time and process) methodology, and through corporate projects also carry out detailed research on what is working here, in other services and also in other sectors to establish what 'good looks like'. We also challenge ourselves by consulting everyone that works for us on proposed projects, and asking for input into ways we can work smarter to simplify internal systems – so improving efficiency for the internal customer, and (via the time saved) to the external customer too.

Performance and data – key action areas

There are eight major areas we need to consider in relation to data and performance in the life of this Strategy. These are:

Approach to transparency

There will remain an expectation that more information will be published on our website, and made generally available to the public to see how we are performing. We will continue to comply with the relevant transparency regulations in the year in question. However we will strive to publish not only the mandatory requirements, but also the voluntary elements of data. We remain of the view that providing incident-level datasets via the website is inappropriate and contravenes the existing legislation on data protection. Aggregated data only will be routinely published.

Actions

- Publish the mandatory and voluntary elements of the transparency code for local government for the relevant year;
- Invite a further audit of the Authority's approach to transparency in 2020.

Response to the General Data Protection Regulations

We will change the relevant policy framework documentation to ensure compliance with the General Data Protection Regulations. We will commission a gap analysis to assess what work needs to be completed. Where this cannot be put in place by 28 May 2018, a clear statement will be made to the public on when it will be fully compliant.

We will incorporate the responsibilities of the 'Data Protection Officer' into the role of the Assistant Director, Policy and Performance, who will represent the public in issues of data usage. This is a more cost-effective mechanism for delivering this role than employing a separate member of staff.

Everyone that works for us will receive a base level of training on the General Data Protection Regulations; principles of data protection; and freedom of information, through e-learning. This will be recorded within training records and able to be interrogated by managers. The subject will also be added to induction packages.

Senior officers responsible for data will undertake such continuous professional development as they deem necessary to fulfil their role.

Actions

- Assess the gap analysis and put in place actions to dealing with any issues arising;
- Incorporate the responsibilities of the 'Data Protection Officer' into the role of the Assistant Director, Policy and Performance;
- Commission and deliver new e-learning on the General Data Protection Regulations and Freedom of Information Act.

Freedom of Information (FoI)

All staff will receive refreshed e-learning on FoI and personal responsibility for data. We will maintain a single channel in and out of the organisation for requests for data from any third party, which will be the 'Information Officer' inbox. No data will be released to any third party under any circumstances without discussion first with the Information Officer or a member of the business intelligence team, or a member of Corporate Management Board. The release of any information will be documented.

Actions

- Commission and deliver new e-learning on the General Data Protection Regulations and Freedom of Information Act.

Data quality

People, money and information are extremely valuable resources for any organisation. Data quality is important as it is used in decision-making, to manage services and account for performance within the Authority and to the public and Government.

All employees will ensure that the data they are involved in producing and/or using is sufficiently accurate, valid, reliable, timely, relevant and complete to meet the needs of the Authority, while ensuring data-gathering remains proportionate to the cost of collection. Data-owners have the responsibility for maintaining an effective QA process for the data they hold.

Anyone that works for us who inputs data has a responsibility for inputting it as accurately and as promptly as possible. They also have a responsibility for highlighting to the relevant Section Head or Head of IT and Business Change where they have doubts about the quality of data they are inputting or doubts regarding the data-capture process and the quality of data it produces. In addition, where data is captured from external sources, particularly the internet, they must take care to validate the data quality prior to data entry.

Financial data is subject to rigorous regular audit and scrutiny. Internal audit contribute to the data quality review and improvement process by undertaking a periodic audit of data quality as part of the overall review of corporate governance. The result of this audit is reported to Members.

Over the life of the Strategy, our approach to capturing personal and building-specific data will be changed to eliminate double-keying of data into numerous system. The development of this system is captured in the Prevention and Protection Programme.

Actions

- Deliver the customer and premises risk management project;
- Deliver the payroll and procurement system project.

Data sharing

Sharing data between agencies is becoming increasingly common for the purposes of understanding customer pathways through public services, or for safeguarding cases, or criminal investigation. Where data-sharing is regular, our default position is that it will be shared by secure electronic means. Usually this will mean its transfer across the Kent Public Services Network. Where the third party is not a member of this network, data will be shared by secure email. Paper records and USB drives are not to be used, unless authorised by the Head of IT and Business Change.

No data is to be accepted onto our network from USB drives, unless authorised by the Head of IT and Business Change.

We will remain a signatory to the Kent and Medway Information Sharing Protocol.

Actions

- Document all data-sharing arrangements and maintain a register of agreements. All data-sharing agreements are to be stored in the relevant SharePoint site for the life of the agreement, and a paper copy placed in the Authority's fireproof contracts cupboard.

Data intelligence and evidence-based decision-making

We have invested in the ability to collect, interpret and present the data collected to support decision-making. An example of this is the data packs which underpin emergency cover reviews. Not only does it use our own data, but it also takes in data and intelligence from other sources such as development plans, data from the Office for National Statistics, and the NHS. We will strive to be an exemplar to the sector on the intelligent use of data for the purposes of evaluating the projects and interventions delivered to customers, and in keeping operational, customer and business risk assessments up to date. We will maintain up to date IT systems to enable us to assess our operational and business risks, such as replacing the FSEC toolkit. The Business Intelligence Team will maintain their CPD in the relevant areas to meet the Service's needs.

Actions

- Replace the Authority's emergency cover modelling system;
- Refresh the Authority's Incident Recording System;
- Refresh the countywide customer and business risk assessment alongside any future Safety and Wellbeing Plan.

Project and programme management

Corporate projects are managed at local level by trained project managers, and overseen by sponsors, who are members of Corporate Management Board. Progress on corporate projects is overseen by the Corporate Development Steering Group. Risks, issues and actions will be documented for all corporate projects, something which we recognise we need to improve on from the current position. Project benefits will be mapped and quantified

(as much as possible) at the beginning of the project to inform the development of business cases and support decision-making. Project benefits will have an owner and will be tracked throughout the life of the project. Once delivered, project benefits will be monitored by the business owner.

Whilst we have invested in skills around project and programme management, there is evidence we are not as mature as we would like to be in this field. The Project Management Office will develop its training offer, and seek to encourage more people to undergo the project management apprenticeship scheme currently being piloted.

The nature of Grey Book (uniformed) roles means that opportunities exist for short term secondments into the Project Management Office which turn over frequently. In future, secondments will be linked to projects so that there is no project flux caused by changing officers. Appropriate use will be made of outside contractors to fulfil roles within projects, either as technical advisors or as project managers themselves, so we can build expertise which is unavailable internally. However, project managers will generally be drawn from inside the Service in order to build capacity.

Data collected by the Project Management Office on project and programme performance will be used to support decision-making by Corporate Development Steering Group. The data will also help to identify areas for improvement and to develop plans to address these accordingly.

Corporate Governance

We define corporate governance as “the system by which local authorities direct and control their functions and regulate their local communities”. The concept of Corporate Governance exists against a backdrop of two separate, yet inter-related, sources: a legal requirement; and adherence to the principles of good governance contained within a framework developed by the Chartered Institute of Public Finance and Accountancy (CIPFA). In short, the legal requirement states what authorities must do in relation to good governance, while the CIPFA framework (“the Framework”) states how they should meet the legal requirements.

Legal requirements

The legal requirement to provide a system of good governance is set out within sections 3 and 6 of the Accounts and Audit (England) Regulations 2015 (“the Regulations”). Section 3 requires an authority to have a sound system of internal control which:

(a) facilitates the effective exercise of its functions and the achievement of its aims and objectives;

(b) ensures that the financial and operational management of the Authority is effective; and

(c) includes effective arrangements for the management of risk.

Section 6 of the Regulations requires an authority to conduct an annual review of the effectiveness of the system of internal control and a statement reporting on the review (to be published at the same time as the Statement of Accounts). The Regulations state that the publication of an Annual Governance Statement (AGS) in accordance with the principles of the CIPFA Framework would fulfil these statutory requirements. We publish this document each year for the summer Authority meeting, and will continue to do so. We will look to simplify our approach to displaying the information contained in the AGS to the public.

The CIPFA Framework

The CIPFA Framework ('Delivering Good Governance in Local Government Framework, 2016 Edition') defines seven principles that should underpin the governance of local government organisations, and provides a structure to aid authorities in their approach to governance and compliance with the legal requirements of the Regulations.

The seven principles are as follows:

Principle A	Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law.
Principle B	Ensuring openness and comprehensive stakeholder engagement.
Principle C	Defining outcomes in terms of sustainable economic, social and environmental benefits.
Principle D	Determining the interventions necessary to optimise the achievement of the intended outcomes.
Principle E	Developing the authority's capacity, including the capability of its leadership and the individuals within it.
Principle F	Managing risks and performance through robust internal control and strong public financial management.
Principle G	Implementing good practices in transparency, reporting and audit to deliver effective accountability.

The Framework states that each local authority should be able to demonstrate that its governance structures comply with the seven principles. In order to achieve this, a local authority should develop and maintain a local code of governance that reflects these principles. For us, this requirement is met through the publication of the Code of Corporate Governance (CCG). This outlines how we will:

(a) Meet each of the seven principles;

(b) Deliver the ability to meet each of the seven principles;

(c) Evidence that we have met each of the seven principles.

The CCG outlines the key systems and controls in place and covers all of the main areas, including service delivery, financial management, and the democratic process.

In November 2016, we published a revised CCG to reflect the changes introduced by the publication by CIPFA of a revised Governance Framework. This will be reviewed within the life of this Strategy, or if the Code changes.

The Annual Governance Statement (AGS)

The AGS provides an overview of the procedures in place and an assessment of the extent to which the Authority is operating effectively to ensure compliance with the CCG and ensure good governance across the Authority. The overall aim of the AGS is to offer effective scrutiny and accountability by providing the public and Authority Members with a clear statement of the processes by which we manage our activities and a degree of assurance that these activities function properly.

In 2012, the Government issued guidance setting out how fire and rescue authorities should extend the annual AGS to include an operational assessment (Operational Assurance Statement) of progress in meeting the Fire and Rescue National Framework (which sets out the Government's priorities and objectives for fire and rescue authorities in England). This Operational Assurance Statement is incorporated into the AGS and published as a single document in two clearly marked sections.

Action plan

- Simplify the Authority's approach to producing its annual governance assurance statement.

Action Plan

Action	Owner	Time scale
Publish the mandatory and voluntary elements of the transparency code for local government for the relevant year.	AD P&P	Annually by June each year
Invite a further audit of the Authority's approach to transparency in 2020.	AD P&P	March 2021
Assess the gap analysis and put in place actions to deal with any issues arising.	AD P&P	May 2018
Incorporate the responsibilities of the data protection officer into the role of the AD P&P.	AD P&P	May 2018
Commission and deliver new e-learning on GDPR and FOI.	AD P&P	March 2019
Deliver the customer and premises risk management project.	Dir Ops	April 2019
Deliver the payroll and procurement system project.	AD Finance	Sept 2018
Document all data-sharing arrangements and maintain a register of agreements. All data-sharing agreements are to be stored in the relevant SharePoint site for the life of the agreement, and a paper copy placed in the Authority's fireproof contracts cupboard.	AD P&P	March 2019
Replace the Authority's emergency cover modelling system.	AD P&P	June 2019
Refresh the Authority's Incident Recording System.	AD P&P	Nov 2018
Refresh the countywide customer and business risk assessment alongside any future Safety and Wellbeing Plan.	AD P&P	Alongside next Safety and Wellbeing Plan
Simplify the Authority's approach to producing its annual Governance Assurance Statement.	AD P&P	June 2019

This page has been deliberately left blank