Wyre Forest District Council

Data Quality Policy

Updated November 2017

Content

Introduction

Aim of the Policy

1. The aim of this Policy is to set out a clear framework for maintaining and improving high levels of data quality within Wyre Forest District Council.

Background

2. The Council recognises that high quality data* (see definition below) is essential for:
   - ensuring the delivery of services against agreed plans
   - Meeting legislative and regulatory requirements
   - Supporting policy formation and managerial decision-making
   - Providing protection and support in litigation including management of risks
   - Providing evidence of business activity
   - Improving efficiency, performance and accountability
   - Supporting business continuity in the event of a disaster

3. The Council has developed this Policy to ensure that the data it produces and uses is of high quality, and to provide a framework for maintaining and improving data quality within the Council.

Scope

4. This Policy applies to all Council Members and employees, and to all information systems owned, used or managed by the Council in paper or electronic media. Guidance Notes for employees will be available on the Council's intranet.

Data Quality

Definitions

5. For the purposes of this Policy, 'data' is defined as 'factual verbal or numerical information which is held by the Council, which may be used to assist decision-making and which can be stored and processed by any medium'.

6. * Data is regarded as being of high quality if it is:

   - Accurate (in terms of correctness)
   - Comprehensive (in terms of all relevant data being captured)
   - Valid (in an agreed format which conforms to any recognised national standards)
   - Timely (available when required)
   - Stored securely and, when required, confidentially

Roles & Responsibilities

7. The Chief Executive has overall strategic responsibility for Data Quality although the operation functions for promoting and co-ordinating this Data Quality Policy and associated procedures, guidance and training sit with the Business Improvement Officer. These duties include:

   - raising awareness of data quality within the Council
   - ensuring security and back-up of the Pentana Performance System
   - follow up of any issues arising from data quality checks
   - checking and monitoring performance information produced by the Council
   - ensuring that training and awareness programmes are used to ensure that all employees and Members are aware of the importance of maintaining a high quality of data

8. Each Director is responsible for ensuring that data generated, used and supplied by their service teams is of a high quality. They will ensure that individual responsibilities and accountabilities for ensuring data quality have been assigned and are regularly reviewed and assessed including via My Development Review Scheme, Generic Competency Framework and Management Competency Framework.

9. Where Members or employees become aware of data quality issues which cannot be immediately rectified and which affect information on which the Council or other organisations are relying, the relevant Director or the Business Improvement Officer will be notified accordingly in order that remedial action can be taken as required.

10. Nominated officers are assigned responsibility for collecting and reporting data on the Pentana Performance System and in other performance reports.

11. Employees are made aware of any measures to which they contribute data and must adhere to agreed procedures for producing, checking and reporting such data.

12. **All employees are responsible for ensuring that data which they create, receive or act upon is of a high quality.**

13. All Members and employees have access to this Policy and associated guidance, which are available on the Council’s Intranet.

Data Quality Monitoring

14. Data quality is monitored by the Business Improvement Officer in accordance with agreed corporate procedures. These include:

- Regular reports
- Routine checks
- Sample checks
- Follow up with remedial action as required and reported to Members

15. Procedures for data capture, processing and storage are reviewed and updated annually. These include specific arrangements for ensuring data quality at the point of data capture, during the processing of that data and appropriate data quality checks before data/information is released.

16. Systems operate on a ‘right first time’ principle in order to avoid the need for routine data cleansing or manipulation to produce the information required.

Internal Control & Validation

17. All systems and procedures have built-in controls to minimise the scope for human error, manipulation or other factors affecting data accuracy (e.g. the use of system validation on key data entries or drop down menus/pick-lists).

18. When data is produced or loaded onto electronic systems the accuracy is to be checked and the data ‘signed-off’ by an authorised officer. If the data inputter is not the officer responsible for this data, it is the responsibility of the owner of the data, e.g. line manager / data manager, to check and validate the data and ensure that it has been loaded correctly.

19. Wherever possible, data should be stored centrally and not duplicated in multiple locations in order to reduce officer time and risk of errors.

Reporting Arrangements

20. These include, but are not limited to:

- The Council
- Cabinet
- Scrutiny Committees
- Corporate Leadership Team
- Directorate Management Teams

21. Data quality reports are prepared on an exception basis so that areas where action is needed are clearly identified. Reports will include an assessment of the risks associated with unreliable and inaccurate data and are included as appropriate in the Risk Register.

Security & Confidentiality

22. The Council is committed to keeping data secure and, where required, confidential in accordance with its Data Protection Policy and other supporting statements and policies, which are available on the Council's intranet and website.

23. Each service team ensures that appropriate measures are taken to ensure the security of its business-critical data systems. Such measures are documented and regularly tested and reviewed. Any areas of concern or weakness are documented and rectified.

24. A Business Continuity Plan is in place to protect records and data which are vital to the effective functioning of the Council. When sharing data with third parties (e.g. partner organisations) protocols are agreed to ensure the quality of the data shared. This will include as a minimum:

- Formal Information Sharing Protocols to ensure that information can be shared lawfully and within the framework of relevant legislation
- An agreed set of standards for the quality of all data shared and the creation of processes to validate the quality of data obtained from third parties