The University of Kent

Corporate Standards for data quality and the collation of data for external presentation

This paper introduces a set of standards with the aim of safeguarding the University’s position in published information, while at the same time building confidence in data and its robustness for analysis. These standards apply to quantitative as well as qualitative (textural) data held in university-wide systems and submitted externally.

The Audit Commission’s publication ‘Improving information to support decision making: standards for better quality data’ (2007) is acknowledged.

Context

A specific objective that targets data quality in isolation is unlikely to result in high quality data. Such quality is the outcome of a seamless process of an organisation’s operational and performance management and governance arrangements.

In particular the processes for independent data review and signoff of all externally transmitted data, procedure notes, audit, resilience and backup, together with staff training and setting clear responsibilities will all contribute to creating the appropriate culture within which data accuracy has a visible importance and can flourish. It is from such a culture that high data quality results.

In applying these standards, heads of Professional Service Departments will need to consider the risk, including the potential future risk, of data in individual returns impacting on the University’s reputation and/or finances. Returns with a high risk will require a higher level of management and scrutiny than those with low risk.

Governance and Leadership

Although Council hold ultimate responsibility for data quality assurance, it is the day-to-day responsibility of individual members of staff to ensure that the principles of this policy are followed to maximise the accuracy and timeliness of data returned externally.

The University will require a culture that demonstrates a high commitment to data quality at a senior level. A culture derives from a strong organisational lead supported by a sound organisational model. Three principles should dominate this commitment:

- That the University should publish a Corporate Standards for Data Quality policy that demonstrates a clear commitment to a culture of data quality throughout the University.
- Strategic responsibility for data quality should be part of the formal portfolio of a member of the Executive Group (EG).
- An objective that all data and data returns should aim for the highest possible standards of accuracy should be established to set a clear expectation of the standards required by the Executive Group.

All users of statistical data held on University systems should be aware of the key principles of data processing contained in the Data Protection Act (1998).
Corporate Objectives for Data Quality

The University of Kent will process data in accordance with Schedule 1 of the Data Protection Act (Appendix 1) and, in the context of this policy, issues of relevance, timeliness and validity are particularly pertinent.

The University of Kent, in common with other Universities, needs complete, accurate and reliable information in order to manage its business, including:

- Delivering an efficient service to staff, students and stakeholders
- Providing informative and reliable management information and reporting
- Demonstrating public accountability
- Presenting a responsible and true public face.

The principal reasons why data supplied externally by the University should be of the highest possible quality are:

- The external presentation of the University has assumed greater significance in the context of increased tuition fees. Potential applicants, their parents and their advisors look increasingly to the performance of the University across a range of statistics in deciding whether to invest significant sums of money. Our performance is compared with our peers, so it is vitally important that the University’s external image, as reflected in the data published about us (that feeds these comparisons), shows the University in the best possible light.

- To ensure accurate funding allocations for both teaching and research (data supplied by the University to HEFCE and HESA affects the funding that the University receives).

- With the increasing reliance on performance management and assessment regimes, it is important to be able to demonstrate the reliability and robustness of the underlying data.

- Good quality data and external data returns reflects a well-run institution and this is likely to influence the University’s external credibility.

- The HEFCE Model Financial Memorandum between HEFCE and institutions (HEFCE 2010/19, Annex B) introduced a new requirement for the Audit Committee to give, as part of its annual opinion, assurance over management and quality assurance of data submitted to HESA and to HEFCE and other funding bodies.

Data Scrutiny & Review

- The need for data items should be periodically reviewed to ensure the data is necessary and that it is collected in the most efficient form.

- Wherever possible, data held on university systems should be:
  - subject to on-line validation at the point of entry;
  - subject to verification by the data subject (where appropriate).

- All data held on University systems should be scrutinised on an on-going basis for reasonableness, accuracy and fitness for purpose with extensive exception reporting to identify possible data errors or missing values.
• Compilers of external returns should pay particular attention to the following:
  
  o Completeness of data sets and missing data issues;
  o Time series / data trends, as an aid to understanding context;
  o Critical appraisal of data abnormalities with explanations documented.
  o The need to consult other relevant departments and individuals to gain necessary consensus before finalising the return.

Independent review

• A thorough assessment of data to be returned externally should be undertaken by a senior person not involved in the collation of the return – preferably a Professional Service Department Head or equivalent.

• The relevant head of a Professional Service Department should evaluate summary statistics for each set of data returned externally:
  
  o for reasonableness;
  o for context in terms of summary statistics for previously submitted data.

• Help should be solicited from an appropriate office (i.e. Planning and Business Information Office) should the necessary technical skills to undertake this work, not be available to a Professional Service Department Head.

Final review and signoff

• As a minimum, the EG member responsible for the appropriate Professional Service Department will then undertake a high level check for credibility and reasonableness before signing off the data return.

Procedure notes

• Procedure notes should inform each external return - periodically updated to reflect most recent instruction and practice.

• Professional Service Heads should ensure that all such procedures are adopted and embedded within working processes to achieve compliance.

Resilience and Backup

• Organisational resilience should be delivered through ensuring that each data return can be compiled by a least two competent and fully trained members of staff – preferably each with practical experience of undertaking the return – thereby minimising the exposure to risk in the event of staff unavailability.

Staff training and Setting Data Responsibilities

• Staff responsible for undertaking data returns should be appropriately trained in the necessary technical skills to undertake the work as well as having an understanding of the context and specifics of the return.

• Responsibilities for data accuracy should be included in job descriptions for those staff with significant management responsibility or where data handling forms an important part of the role.
• All members of staff should understand their role in contributing to good quality data as well as their individual responsibilities and be aware of the implications of poor data quality both within the institution and externally.

• Members of staff should be encouraged to report immediately to their manager if data quality issues are identified. The manager will undertake appropriate action to remedy the situation.

Audit and Reporting

• Each occurrence of the external submission of data should demonstrate transparency between summary statistics derived from the data to be reported externally, and the summary data set held in internal systems, with a full reconciliation analysis for any differences for each return.

• Each external return should be supported by a document setting out a clear, complete and verifiable audit trail. It should also enable confirmation that the methodology employed meets relevant requirements.

• Internal audit will carry out work to support the Audit Committee’s requirement to report as part of its annual opinion on the management and quality assurance of data. This work will include a consideration of the application of these standards and a review of selected returns.

• The DVC with responsibility for the ‘Corporate Standards for Data Quality’ will report annually to Audit Committee. The content of this report will inform the University’s risk management process.

• Heads of Professional Service Departments will be required to maintain a risk assessed list of external data returns undertaken by their department and report annually to the chair of Council in order to inform the risk management process.

• All external returns should comply with the Corporate Standards for Data Quality.

• For high risk data returns, a checklist should be completed to provide assurance to the Executive Group member and the University that the return has met the minimum standards implied by the Corporate Standards for Data Quality

• A periodic (biennial) review of the Corporate Standards for Data Accuracy will be undertaken by the Executive Group to ensure that they remain fit for purpose.

Summary of Key Actions

• Each Head of a Professional Service Department should compile and maintain a list of the regular data returns made by his/her Department on behalf of the University, with an indication of the risk generated by each return in terms of reputation.

• Each Professional Service Head should ensure that a set of protocols (in the form of procedure notes) is maintained for each regular external return.
• A summary of each regular external return should be approved by the Executive Group member responsible for the area covered by the return. Additionally the Vice-Chancellor may be required to sign off the return as ‘Head of Institution’.

• Each Professional Service Head should ensure that there is adequate cover in the specialist skills and knowledge necessary to complete each external return.

• Each new external demand for data should be reviewed from a perspective of the external implications and the Executive Group member responsible alerted. This implies that the data return will be summarised and evaluated against previous or similar data returns.

• Data returns, and compliance with this strategy, will form part of the work of the internal Audit Team.

Contact

Advice or questions concerning this policy or issues arising from it, in the first instance, should be addressed to Dr Keith Lampard, Secretary to Council, The Registry, Canterbury CT2 7NZ.

Jco 17/07/13
Appendix 1

Data protection principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.