BREACH OF THE CODE OF PRACTICE FOR OFFICIAL STATISTICS

A breach of the Code of Practice for Official Statistics occurs where one or more provisions of the Code were not followed in situations where an exemption or exception had not been approved by the UK Statistics Authority's Head of Assessment, as required in paragraph (xii) of the Code's preamble.

1   Background Information

Name of Statistical Output (including web link if relevant)

Public Sector Finances First Release (and associated dataset)

Name of Producer Organisation

Office for National Statistics (ONS) and Her Majesty's Treasury (HMT)

Name and contact details of person submitting this report, and date of report

Tom Josephs, Pubic Sector Finances Team, HMT, 2 March 2009

2   Circumstances of Breach

Relevant Principle/Protocol and Practice

Protocol 2, Practice 8 – accidental and wrongful release

Date of occurrence

18 February 2009

Nature of breach (including links with previous breaches, if any)

The public sector finances dataset and first release are joint ONS/HMT products. At 18:19 on 18 February the internal HMT January 2009 public sector finances briefing was accidentally sent in an email to an extensive internal distribution list. The brief is marked "Restricted Statistics" and should not have been sent before 9:30 on 19 February.

Reasons for breach

3   Reactions and Impact

None – there is no evidence to suggest information was released to the public as a result of this incident.

4   Corrective Actions Taken (include short-term actions, and long-term changes made to procedures)

The email was recalled at 18:21. Everybody that had already opened the email was emailed again, telling them to delete the email and with a message explaining that email contained restricted National Statistics. The only recipient outside of HMT was telephoned and informed to do likewise.. The National Statistician was informed. We have reviewed our administrative procedures for handling the briefing email. We have put in place a new system with additional safety checks to ensure this cannot happen again.

5   Any other relevant supporting material (including link to published statements about this breach)