# BREACH OF THE CODE OF PRACTICE FOR OFFICIAL STATISTICS

This document reports a breach of the Code of Practice for Official Statistics, or the relevant Pre-release Access to Official Statistics Orders, to which the Code applies as if it included these orders.

## 1. Background information

Name of Statistical Output (including weblink to the relevant output or 'landing page')

Foreign Direct Investment - Annual Inwards 2011 (non-market sensitive):

http://www.ons.gov.uk/ons/rel/fdi/foreign-direct-investment/2011-sb/stb-fdi-2011.html

Mergers and Acquisitions - Q1 2013 (non-market sensitive):

http:/www.ons.gov.uk/ons/rel/international-transactions/mergers-and-acquisitions-involving-uk-companies/q4-2012/stb-m-a-q4-2012.html

Name of Producer Organisation

Office for National Statistics (ONS)

Name and contact details of the statistical Head of Profession (Lead Official in an Arm's Length Body) submitting this report, and date of report

Glen Watson, Director General (DG), ONS,

Email: dg@ons.gsi.gov.uk

Tel: 01633 655252

## 2. Circumstances of breach

Relevant Principle/Protocol and Practice

**Principle 5: Confidentiality**
"Private information about individual persons (including bodies corporate) compiled in the production of official statistics is confidential, and should be used for statistical purposes only".

**Practice 2:** "Keep confidential information secure. Only permit its use by trained staff who have signed a declaration covering their obligations under this Code.
information during normal working hours."

Date of occurrence

The breach took place on 16th April 2013.

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

On 16/04/2013 at 6.23pm an ONS employee sent disclosive microdata to 2 external email addresses of an ex-ONS contractor. This was part of an exercise to fix and test a piece of code associated with an electronic data collection instrument that the contractor had previously developed. The contractor had agreed to provide ONS with consultancy support on this code in the run up to releasing it into production.

The files that were sent contained individual company data for all the Foreign Direct Investment variables that are collected by the survey (44 questions describing an individual company business structure and their balance sheet figures). The file contained 15 individual company records.

The same ONS employee sent a further email on 17/04/13 at 1.58pm. This contained a file with approximately 15,000 rows of individual company level data for the Foreign Direct Investment survey variables (44 questions describing an individual company's business structure and their balance sheet figures) and also data for the Mergers and Acquisitions survey variables (describing an individual company's business structure and the acquisition deal figures).

The ONS employee immediately realised that the second email contained disclosive data (and on reflection so did the first email). As such, the ONS employee took immediate action and notified their line manager of this security breach and potential breach of the Code of Practice for Official Statistics. In turn, the Grade 7 and Deputy Director were notified immediately.

The second email on 17/04/13 at 1.58pm failed to deliver due to its size and did not leave ONS. However, at the time of management notification this was not known.

Reasons for breach

The files were originally supposed to contain dummy data and were being sent to explain the format of the datasets. For this reason, the files were not marked as "RESTRICTED" and were sent to a personal email address. However, the ONS employee accidentally placed real data from the live system into these files and sent them to the ex-ONS contractor without realising.

**3. Reactions and impact (both within the producer body and outside)**

We have not received any internal complaints around this breach. We are not aware of any external reaction from outside bodies or from within the media.

**4. Corrective actions taken to prevent reoccurrence of such a breach (include short-term actions, and long-term changes made to procedures)**

The following individuals were contacted by email and telephone so that a collective ONS 'line to take' could be ascertained:

- Head of International Transactions branch, Business Outputs and Developments Division
- Deputy Director, Business Outputs and Developments Division
- Senior representative of DG office
- Head of Legal Services
- Head of Information Assurance

**Short term corrective actions:**

1) Deputy director of Business Outputs and Developments division informed Head of Collection and Production Directorate of the breach.

2) Head of International Transactions branch contacted the ex-ONS contractor to confirm the deletion of the emails and obtained a statement confirming the following:

- All files have been deleted from all email accounts;
- All files have not been downloaded onto a PC or any other hardware;
- In the event that above occurred, that all files have now been deleted;
- The files have not been passed on to anyone else either electronically of via paper copies;
- That if the files are accidentally restored (i.e. via undo, refresh, system restore) in the future they will be immediately deleted.

This was confirmed with the ex-ONS contractor.

3) Head of International Transactions branch contacted Legal Services, Director General office and Information Assurance to alert them to the breach.

4) Head of International Transactions branch filled in the 'Breach of Code of Practice' template outlining what happened, action taken etc.

5) Deputy Director, Business Outputs and Developments division wrote to all staff within the Division raising awareness of the incident, reiterating the critical importance of keeping respondent information secure and ensuring that such information should not be sent via email.

**Further corrective actions (with 2 weeks, or as specified):**

6) Head of International Transactions branch made the ONS employee aware of the breach and explained why this was the case.

7) Head of International Transactions branch established whether the ONS employee had received security training and signed a declaration covering their obligations under the Code of Practice, to which the answer was 'Yes' in both cases. Head of International Transactions branch reviewed security training with ONS employee.

8) Head of International Transactions branch cascaded to department to be very mindful of

security and the transmission of data and reviewed and enhanced the current internal guidance.

9) Head of International Transactions branch coordinated further quality assurance measures by further restricting access to Live IT system

10) Head of International Transactions branch to send out reminders on a monthly basis that all internal and external data transmissions must be quality assured by the Head of International Transactions branch.

11) Deputy director of Business Outputs and Developments division to continue drawing attention to the need to be mindful of security during divisional cascades and ensure ongoing enforcement of mandatory "protecting information" online training - ongoing.

12) Circulate important reminder across the office from a Corporate Level highlighting the policy for sending data via email and following the appropriate security protocols - End April.

**Corporate action:**

13) Details of the breach will be submitted to the ONS Board. The corrective actions are being tracked to closure by the business area and the corporate centre..