Statement of confidentiality

Objective

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

Code of Practice for Official Statistics, January 2009.

ORR has outlined below how we observe the principles outlined in the confidentiality protocol. This has been broken down into the following sections:

- security procedures;
- organisation security;
- organisation training;
- security markings; and
- publishing procedure.

Following this ORR has included a summary of tables published by ORR which shows how ORR publishes the data in such a way as to ensure confidentiality is protected and used for statistical purposes only.

Security procures

Physical security

ORR conforms to the physical security requirements as specified in the security framework (available on the Cabinet office website) based on a risk approach. Some examples include:

- All staff and visitors must be registered to enter the building in order to pass security; there is no public access to the building.

- Visitor must wear visitor badges at all times and must be accompanied at all times. Visitors are not allowed within the main ORR working area and are only allowed access to the ORR meeting rooms which are in a separate part of the office.

- ORR office floors have security doors which only staff can unlock with their pass.

ORR publishes security manuals which detail the individual responsibilities and procedures to provide an adequate level of protection for people and information, this is available internally on ORR's intranet.

Computer username and passwords

All computers require a username and password to login; passwords are changed regularly and must be of a suitable strength.

Technical security

ORR operates within the Government Secure Intranet (GSI) and will continue to adhere to and monitor the relevant compliance standards.

All ORR issued laptops are encrypted.

Organisation security

The following individuals have specific responsibility for security at ORR:

(a) Senior information risk owner (SIRO) – Lynda Rollason
(b) Departmental security officer (DSO) – David Phillips
(c) IT security officer (ITSO) – Richard Hope
(d) Head of information management and data protection officer – Jenny Godfrey

Information asset owner (IAO)

There are a number of IAO's at ORR who can give advice on confidentiality issues with data. Each department has a designated IAO who is responsible for understanding what information is held and understand and address potential risks to the information.

ORR guidance material

ORR has a comprehensive Information security policy which covers how we ensure the confidentiality, integrity and availability of ORR's information. This covers emails, documents, records and data in electronic and paper form, as well as our computer applications and systems.

Internal storage

Information is held within a local folder stored on a server and can only be accessed by the relevant staff set-up by ORR information services team.

Organisation training

Data protection training

As part of the government information security responsibilities ORR staff are required to complete level 1 of the National School of Government's Protecting Information e-learning module.

Code of practice training

The information and analysis (I&A) team has carried out a campaign to raise awareness of the code of practice and how this affects staff inside ORR, such as how to deal with sensitive data prior to publication. The I&A team conveyed this message through using a number of methods such as bite size seminars, one-to-one meetings, internal guidance and intranet guidance.

The bite size seminars are planned to run every year and will be used to induct new staff or as a refresher course to present staff.

Security markings

Pre-release

ORR is compliant with the pre-release order; this ensures we protect data from being released prior to publication. Please read our pre-release compliance statement for further detail on this.

Security markings

ORR follows the Government protective marking system to ensure sensitive material is appropriate marked. ORR statistics have been labelled at *Protect* level by ORR's information management team. An example of a security marking is shown below:

For people on the ORR's pre-release list

PROTECTED STATISTICS - DO NOT PASS ON TO PEOPLE NOT ON THE ORR PRE-RELEASE LIST

Access terms for people on the ORR pre-release list

These are official statistics to which you have privileged access in advance of release. Please prevent inappropriate use by treating this information as restricted since this document is intended for people only on ORR's pre-release access list. If you do forward this document to people not on the pre-release list you will be removed immediately. If you feel a colleague will provide added expertise to this document prior to official publication you must get authorisation from ORR rail statistics team. If you no longer require pre-

release access please notify the ORR stats team and you will be removed from the list.

For internal use of unpublished statistics

PROTECTED ORR STATISTICS: THESE ARE UNPUBLISHED DATA AND FOR INTERNAL USE ONLY.

Access terms for people who receive unpublished data

These are internal ORR statistics to which you have privileged access in advance of publication. Please prevent inappropriate use by treating this information as restricted since this document is intended as briefing data for internal ORR use and should not be distributed. This is a requirement under the National Statistics Code of Practice and any breach of this will be reported to ORR's Head of Profession for statistics.

ORR has internal guidelines for how this should be managed and this was covered for ORR's code of practice bitesize seminars and documentation is available on ORR's intranet to all staff.

Publishing data

Protecting the identity of individual or organisations

ORR ensures that publication of statistics are presented in such a way so the identify of organisations or individuals can not identified and are used exclusively for statistical purposes.

It is essential for ORR to protect confidential data since the data is provided to us with the expectation that the information will be kept out of the public domain.

See annex A for specific examples for how this is observed within ORR.

Third party sharing of data

Contractors, consultants, researchers and other third party individuals who may have access to handle sensitive data are required to sign a declaration of confidentiality, see annex C. All requests must be approved by the department's Head of Profession and will normally form part of the contract or service level agreement between ORR and the third party for a particular set of work.

FOI requests

ORR has a team specifically to deal with FOI requests to ensure ORR does not disclose confidential data whilst meeting the requirements under the FOI

act. The FOI team also provides guidance and training to ORR staff on FOI matters.

Annex A: Summary of data within ORR and steps taken by ORR to ensure non-discloser of sensitive material

National rail trends

Chapter	Table	Source	Current level of publication.	Does ORR handle any data that could be classified at 'protect' level for this chapter. If yes, how is confidentiality of data kept.
1	1.1 to 1.3 – Passenger km, journeys and revenue	LENNON database and ATOC	Publish at an aggregated level, either by ticket type or at sector level.	The Lennon system contains sensitive data at TOC level. ORR aggregates the data to sector level and by ticket type to avoid TOCs being identified.
	1.4 TTKM	ATOC	Publish by TOC	No
2	2.1 PPM	Network Rail	Publish by TOC	No
	2.2 Complaints	Department for Transport	Publish by TOC	No
	2.3 NRES	Department for Transport	By type of service.	No
	2.4 PIXC	Department for Transport	By TOC.	No. ORR only receives final figures.
3	3.1 Freight moved	Network Rail	By type of freight commodity.	Yes – data is sensitive at individual freight operating company (FOC) level. We aggregate the FOCs figures into one total so individual companies can not be identified.
	3.2 Freight lifted	Separate FOCs	By coal and other	Yes – individual FOC data is

				sensitive. We aggregate the FOCs figures into one total so individual freight companies can not be identified.
4	National Passenger Survey (NPS)	Summary	Publish a summary of NPS report.	No
5	Fares	By ticket type and sector	By ticket type	The Lennon system is used which contains sensitive data. The data is supplied by external suppliers who are responsible for managing the database. The data is confidential at TOC level. ORR publishes by ticket type to avoid TOCs being identified.
6	6.1 Average age of rolling stock	Department for Transport	By sector	No – we receive the final figures from DfT.
	6.2 Government support to the rail industry	Department for Transport		No
	6.3 Investment in the rail industry	Office of National Statistics	By type of investment	Yes, the data is sensitive at individual company level and ORR will not disclose what companies are included within the survey. We only publish at aggregate level by type of investment.
	6.4 Infrastructure on the railways	Network rail	Infrastructure categories	No
7	Regional usage	Historical Rail Database (HRD)	By TOC	Yes, the lowest level we can publish the data is at regional level. Publishing at regional level protects train companies data from being revealed and this format is agreed with the Association of Train

				Operating Companies (ATOC).
8	Train Operating Companies			No.
9	Sustainable development			No.
10	Safety data	SIGNAL		SIGNAL database contains sensitive data. All data is made anonymous prior to publication.

Annex B: Observing confidentiality requirements with ORR's administrative tools

This annex gives a summary of the main administrative tools and databases used within ORR for statistical purposes. The annex gives a brief followed by steps taken to ensure ORR does not release disclosive statistics.

1) LENNON (Latest Earnings Networked Nationally Over Night)

In accordance with the GSS/GSR disclosure policy for tables produced from administration data sources[1] ORR has identified the data outputs as a low risk category, since ORR publishes the data at a high level of aggregation and are only produced from one database. ORR therefore feels the likelihood of a train operating company being identified from tables 1a to 1c are low. ORR believes the aggregated sector level (London and South East, regional and long distance) and by ticket type (Ordinary fares, season tickets and by non-franchised) is suitable for the rail industry.

Steps for ensuring access to non-disclosive statistics

Users requirements for the published statistics	Users are required to view quarterly data on passenger kilometres, journeys and revenue. ORR aggregates this data by sector and ticket level. Sector level tables are split into long-distance, London and south east operators and regional operators. Ticket types are split by ordinary fares and season ticket fares.
Key characteristics of the data	The data is downloaded from the lennon database. Lennon is the ticketing system for the rail industry. A primary role of lennon is to distribute money from railway tickets to various train operating companies.
Circumstances where disclosure is likely to occur?	The data would be disclosive if train operating companies could be identified.
Disclosure control methods	To risk of train operating companies being identified or being made identifiable is low since we aggregate the data into sectors and by ticket level.

[1] *GSS / GSR disclosure control policy for tables produced from administration data sources*, **http://www.knowledgenetwork.gsi.gov.uk/statnet/statnet.nsf/RefDocs/DBHL-6ZYFQN?OpenDocument**, accessed 25-08-09

2) Historical Rail Database (HRD)

The HRD consists of origin-destination data for journeys, revenue and kilometres travelled by passengers on the national train network.

Steps for ensuring access to non-disclosive statistics

Users requirements for the published statistics	Users are required to view origin and destination data for journeys, revenue and passenger kilometres between different regions.
Key characteristics of the data	The data is originally derived from the LENNON database. The data is supplied to ORR and uploaded a contractor. There are sufficient confidentiality agreements in place. ORR accesses the data via the Historical Rail Database.
Circumstances where disclosure is likely to occur?	Disclosure can occur if a breakdown lower than regional level is distributed. This is because individual train operating companies may be able to be identified at a lower level than regional level, we therefore are only authorised by ATOC to publish at regional level. Occasionally ORR receives ad-hoc requests asking for a lower level of breakdown than regional level. ORR can not supply data which is at a lower level than regional level due to the commercial sensitivity of the data. ATOC have provided ORR with guidelines for what ORR can and can not publish.
Disclosure control methods	In accordance with the *GSS / GSR disclosure control policy t*he current data output within NRT is currently at a low risk of identification since the data is published at regional level so individual train companies and specific routes can not be identified.

3) Investment survey

The investment survey, table 6.3a and 6.3b within NRT, is currently contracted out to the Office of National Statistics (ONS). The survey asks private companies about their investment in the rail industry. ONS are responsible for informing the companies how their confidentiality with be protected and how ORR will publish the data. All of this is detailed in a service level agreement between ONS and ORR.

Company data is confidential since those companies who return financial information expect the information will be kept out of the public domain. Companies are informed directly about the purpose of the investment survey and ORR's use of the data. The following line is used within the investment survey which informs users that ORR will keep the data confidential:

'All the information you provide is kept strictly confidential. It is illegal for us to reveal your data or identity your business to unauthorised persons'

ORR receives data for each private company from ONS to enable ORR to validate and check the data for accuracy. The file is sent by ONS using a password protected excel sheet to the person named within the service level agreement. The password is changed regularly and is sent separate from the data e-mail. The data is stored within ORR's storage system and is password protected. ORR does not publish individual level company information and only publish at a aggregated level.

Users requirements for the published statistics	Users are required to view a total of investment in the railway industry each quarter broken down by type of investment.
Key characteristics of the data	The investment survey is managed by ONS. Every quarter a survey is sent to upto 40 private companies and asks for their investment in the previous quarter.
Circumstances where disclosure is likely to occur?	Disclosure could occur if one or more individual company's financial investment could be identified.
Disclosure control methods	ORR aggregates all companies so the likelihood that an individual company's investment could be identified is low. In addition ORR does not disclose the companies involved within the survey.

4) SIGNAL

The collection of data within SIGNAL is compulsory under the Reporting of Injuries, Diseases and Dangerous Occurrences 1995 (RIDDOR) which came into affect from 1 April 1996. Employees are required to report work related deaths, certain injuries resulting from accidents and work related diseases to ORR. ORR is the enforcing authority for health and safety legislation for the railway and its role includes receipt of the reports and publishing the data.

ORR records RIDDOR reports within a database called SIGNAL. Incident reports are collected and the data assigned to the appropriate SIGNAL categories.

Users requirements for the published statistics	Users are required to view yearly health and safety data.
Key characteristics of the data	Various health and safety statistics on the railway network.
Circumstances where disclosure is likely to occur?	If an individual could be identified or personal information was disclosed.
Disclosure control methods	ORR does not publish individual level reports. ORR aggregates data into suitable categories.

Annex C

Declaration of Confidentiality in Official Statistics

[Information and analysis team]

"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."

I have read the above Principle and the confidentiality practice statements in the Code of Practice for Official Statistics.

I will seek the advice of Government Statistical Service colleagues or the guidance of my Head of Profession for Statistics if I am unclear about how to apply this principle in my work.

Where there is doubt about the scope of this Declaration in my work I will seek clarity in writing from my Head of Profession.

In particular, I will ensure:

- Official Statistics do not reveal private information about individuals.
- Data for Official Statistics are used for statistical purposes only.
- Data for Official Statistics data are kept secure.
- Data for Official Statistics are shared only according to written agreements.

I consider myself to be sufficiently well trained to uphold the confidentiality principle in my work. I acknowledge that I do not have the authority to breach these obligations other than with the specific and written instruction of my Head of Profession.

I am: Copy to Head of Profession:

Signature _____ Name _____

Name _____ [HoP contact details]

Date _____

Declaration of Confidentiality in Official Statistics

[3rd party staff]

"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."

I have read the above Principle and the confidentiality practice statements in the Code of Practice for Official Statistics.

I will seek advice from the sources named in the Confidentiality Protection Agreement if I am unclear about how to apply this principle in my work.

Where there is doubt about the scope of this Declaration in my work I will seek clarity in writing from the signatory to the Confidentiality Protection Agreement.

In particular, I will ensure:

- Official Statistics do not reveal private information about individuals.
- Data for Official Statistics are used for statistical purposes only.
- Data for Official Statistics data are kept secure.
- Data for Official Statistics are shared only according to written agreements.

I consider myself to be sufficiently well trained to uphold the confidentiality principle in my work. I acknowledge that I do not have the authority to breach these obligations.

I am:

Copy to signatory to the Confidentiality Protection Agreement:

Signature _____

Name _____

Name _____

[contact details]

Date _____