Statement on data governance and confidentiality

August 2019

Objective

"Organisations should look after people's information securely and manage data in ways that are consistent with the relevant legislation and serve the public good."

Code of Practice for Statistics Edition 2.0, Trustworthiness pillar T6 – data governance, February 2018

In this statement of data governance and confidentiality, ORR has outlined how we adhere to the data governance principles in the Code of Practice, including arrangements for protecting confidential information used for statistical purposes. This has been broken down into the following sections:

- Organisation security procedures
- Data processing and publishing
- Security markings

In **Annex A** there is a summary of the sensitive data held by ORR and how it's collected, stored and published to ensure it is appropriately protected and used for statistical purposes only.

Organisation security procedures and data management

1. ORR has a comprehensive data protection policy which covers how we ensure the security, confidentiality and appropriate use of the information we hold, and sets out how we comply with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA).

2. The following individuals have specific responsibility for security at ORR:

   - Senior information risk owner (SIRO)
   - Departmental security officer (DSO)
   - IT security officer (ITSO)
   - Data protection officer

Information asset owner (IAO)

3. An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. The DSO maintains an Assets and Risk Assessment workbook for ORR with a list of IAOs and the information they own. Each team has a designated IAO who is responsible for understanding what information is held and to understand and address potential risks to the information. Annually, the DSO asks all IAOs to complete a Business Risk Assessment for the information that they own.

Data protection training

4. All ORR staff are required to complete two e-learning modules - Responsibility for Information and GDPR.

Physical security

5. 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

6. 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

7. All computers require a username and password (Windows Authentication) to login. Passwords are changed regularly and must be of a suitable strength.

Technical security

8. All ORR issued laptops are encrypted with a BitLocker key. BitLocker is a Microsoft Windows encryption feature designed to protect data. A key is assigned to each member of ORR staff and is entered onto the laptop before the ORR Windows Authentication.

Data processing and publishing

Internal storage

9. ORR uses a secure cloud content management service for the storage of all business information. All processed data and analysis for the production of official statistics are stored within a secure area of that system, that can only be accessed by designated members of the ORR's Information and Analysis (I&A) team. No data are held on laptops or other portable devices, or kept on unprotected storage media. All storage media devices are password protected.

10. In addition, the I&A team also manages a bespoke data warehouse environment, hosted on the Microsoft Azure cloud platform. The data warehouse is used to store the SQL database from which all data tables published on the ORR data portal are produced. This environment is password protected and can only be accessed by specific members of the I&A team. Access is managed by system administrators and is only granted where a formal request is made by either the Head of Profession or the Business Intelligence Manager

Protecting the identity of individual or organisations

11. For the production of some official statistics ORR has access to detailed personal and organisation specific information that, if released, would likely constitute a breach of either GDPR, DPA or other data sharing agreements. ORR ensures that these

data are used exclusively for statistical purposes and implements disclosure control methods when preparing statistics for publication to ensure data are presented at an appropriate level of aggregation. These are agreed with the data owners such that the organisations or individuals cannot be identified.

12. 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.

13. See **Annex A** for specific examples for how this is observed within ORR.

Third party sharing of data

14. Under standard ORR contract terms, all contractors, consultants, researchers and other third party individuals who may have access to sensitive data on behalf of ORR agree to appropriate safeguarding and declare that they will not disclose any confidential information without written consent. 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.

Freedom of Information (FOI) requests

15. 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.

Code of practice training

16. The I&A team carried out a campaign to raise awareness of the refreshed Code of Practice during 2018 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 presenting at staff briefings, one-to-one meetings and internal guidance notes. Work shadowing has also been offered to members of other teams, e.g. communications staff, and new analysts.

17. The principles of the Code and the working practices used to produce statistics are explained to all ORR staff involved in the production of statistics upon induction. In addition, ORR's Communications team have a clear understanding of how the Code applies to their activities, and new joiners are briefed by a senior statistician.

Security markings

Pre-release

18. ORR is compliant with the pre-release order; this ensures we protect data from being released prior to pre-announced publication dates. Please read our *Statement on Orderly Release and Revisions Policy* for further detail on this.

Security markings

19. ORR follows the Government protective marking system to ensure sensitive material is appropriate marked. Pre-release access to official statistics are labelled as 'OFFICIAL-SENSITIVE', as it has been judged there is a clear and justifiable requirement to reinforce the 'need to know' around these statistics. All pre-release access documents that are shared are appropriately security marked. An example is shown below:

    OFFICIAL-SENSITIVE STATISTICS: Restricted access until 9.30am [publication date]

20. The email and all file names of attachments containing the pre-release material are marked 'OFFICIAL-SENSITIVE'. The body of the email contains the following handling instructions:

For people on the ORR's pre-release list:

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

Handling instructions for people on the ORR pre-release list

These official statistics will be published at 9.30am on *{DAY MONTH YEAR}* and must not be discussed or shared with anyone not on the pre-release access list until they have been published. Any accidental or wrongful release before publication could have damaging consequences and must be reported immediately. Wrongful release includes indications of the content, such as descriptions like 'favourable' or 'unfavourable'.

For internal use of unpublished statistics:

ORR statistics produced from management information and distributed internally for operational purposes prior to the production of their official statistics final form are labelled at 'OFFICIAL' level.

OFFICIAL STATISTICS

Access terms for people who receive unpublished data

These are internal ORR statistics to which you have privileged access. 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.

Annex A: Summary of sensitive data held by ORR and steps taken to ensure non-disclosure

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

1. LENNON (Latest Earnings Networked Nationally Over Night)

Key characteristics of the data	LENNON is the ticketing system for the rail industry, which stores near real-time data on all tickets sold and the associated revenue. A primary role of LENNON is to distribute money from railway tickets to various train operating companies.
Publications used in	• Passenger rail usage • Regional rail usage • Estimates of station usage • Passenger rail service complaints
User requirements for metrics published and level of disaggregation	Passenger journeys/kilometres: • Passenger rail usage – quarterly data published at a train operator level • Regional rail usage – annual data on journeys within/between 10 regions of Great Britain Ticket revenue • Passenger rail usage – quarterly data on ticket revenue by ticket types (ordinary and season ticket) and sector (London and South East, regional, long-distance) Station entries and exits • Estimates of station usage – annual data on the number of passengers entering, exiting, and interchanging at each station on the GB rail network
Circumstances where disclosure is likely to occur?	The level of disaggregation in these publications has been authorised by the data owner, the Rail Delivery Group, as the lowest permissible in order to protect the commercial interest of the train operating companies. The data would be disclosive if revenue information for individual train operating companies could be identified, or if passenger flows between specific stations/areas could be derived.
Disclosure control methods	The risk of confidential data being identified from the published statistics is low since all data is aggregated on secure ORR systems prior to publication.

2. Investment survey

Key characteristics of the data	The investment survey is contracted out to the Office for National Statistics (ONS). Annually the survey asks around 40 private companies about their investment in the rail industry. ONS are responsible for informing the companies how their confidentiality will be protected and how ORR will use and publish the data. This is detailed in a service level agreement between ONS and ORR. 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' Those companies who return financial information therefore have a reasonable expectation that the information will be kept out of the public domain. ORR receives data for each private company from ONS to enable ORR to validate and check the data for accuracy. The data is stored within ORR's storage system.
Publications used in	Rail finance
User requirements for metrics published and level of disaggregation	Total of investment in the railway industry each year broken down by type of investment.
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	The risk of confidential data being identified from the published statistics is low since all data is aggregated on secure ORR systems prior to publication. In addition, ORR does not disclose the companies involved within the survey.

3. RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrence Regulation)

Key characteristics of the data	RIDDOR is a legal requirement on dutyholders to submit personal injury data to ORR as the Health & Safety Regulator for operational railways.
Publications used in	Rail safety statistics
User requirements for metrics published and level of disaggregation	Passenger/Public/Workforce safety – annual number of injuries on mainline, London Underground and non-mainline networks • Injury data by severity of injury (fatal, major, minor, member of public direct to hospital) • Injury data by type of incident (e.g. assault, on-board injury, slips, trips and falls etc.) • Public injury data by person type (e.g. trespasser, level crossing user etc.) • Workforce injury data by person type (e.g. revenue protection officer, train driver etc.)
Circumstances where disclosure is likely to occur?	For legal reasons, the incident reports include personal details including name and contact details of the injured party. Disclosure could occur if individual people could be identified.
Disclosure control methods	The risk of confidential data being identified from the published statistics is low since all data is aggregated on secure ORR systems prior to publication.

4. Freight Volumes

Key characteristics of the data	Freight data is provided by freight operating companies on a quarterly basis and by Network Rail on a periodic (4 weekly) basis, covering the volumes of freight transported on the rail network
Publications used in	Freight rail usage
User requirements for metrics published and level of disaggregation	Freight lifted • Volume of freight lifted (GB total) split between Coal and Other Commodities Freight moved • Volume of freight moved (GB total) split by commodities (e.g. Metals, Construction, Domestic Intermodal, Coal etc.)
Circumstances where disclosure is likely to occur?	The level of disaggregation in these publications has been agreed between the freight operating companies and ORR as lowest permissible in order to protect the commercial interest of the freight operating companies. The data would be disclosive if volume information for individual freight companies could be identified, and could have an adverse effect on the competitiveness of the freight market.
Disclosure control methods	The risk of confidential data being identified from the published statistics is low since all data is aggregated on secure ORR systems prior to publication.

This publication is available on the ORR data portal.

Any enquiries regarding this publication should be sent to us at orr.gov.uk/contact-us.