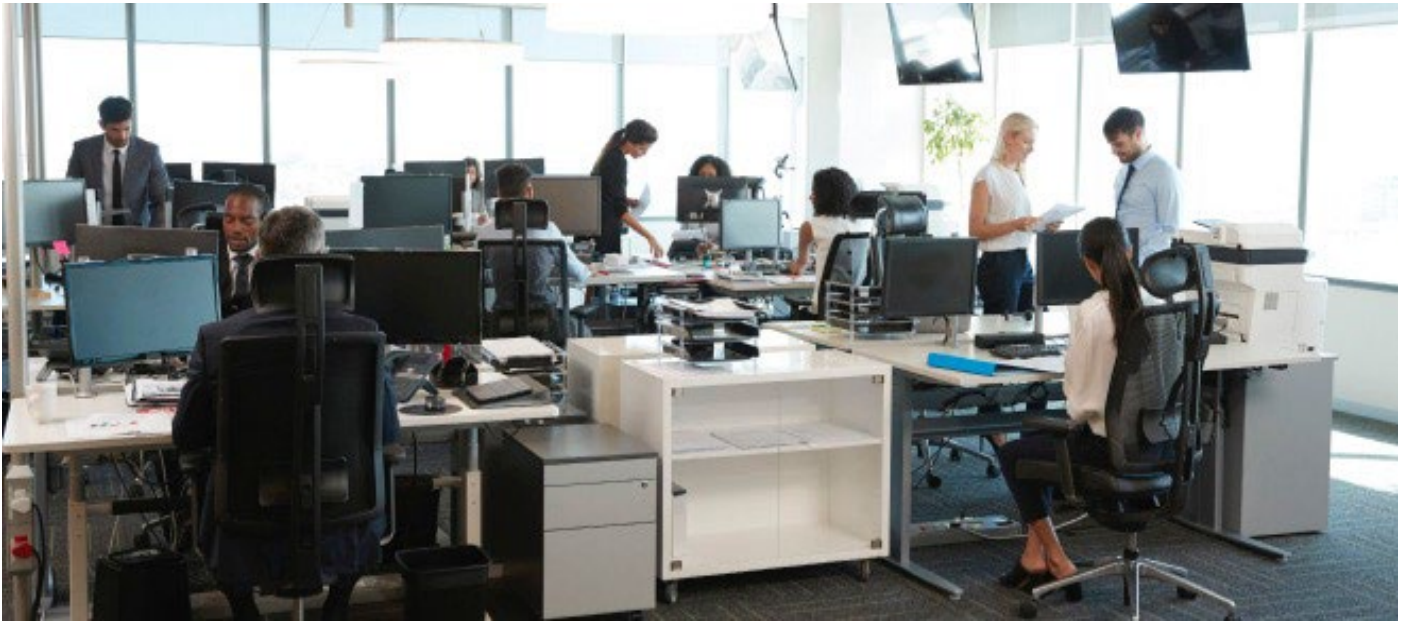


Code of Practice Data Governance and Confidentiality Statement



Issued by:
Workforce Statistics & Analysis
Bruce Street
Belfast BT2 7JD

Last updated: November 2024

Contact: Gayle Kennedy
Telephone: 028 9038 8439

Email: workforcestatisticsandanalysis@finance-ni.gov.uk

Website: [NI Civil Service Human Resource Statistics | Northern Ireland Statistics and Research Agency](#)

Introduction

Workforce Statistics & Analysis is the statistical team embedded within People and Organisational Development within the Department of Finance (DoF) in the Northern Ireland Civil Service (NICS). Consisting of statisticians from the Northern Ireland Statistics & Research Agency (NISRA), we are responsible for producing and disseminating a range of Official and Accredited Official Statistics relating to the HR functions of the NICS, including recruitment, promotion and equality; sickness absence; as well as pay forecasting and Equal Pay Audits. The full series of statistics published by WSA is available on the [WSA section](#) of the NISRA web site.

This Data Governance and Confidentiality Statement sets out the arrangements WSA has put in place to:

- Maintain the trust and co-operation of those who own and manage administrative data sources used by us and persons on our email distribution lists;
- Comply with the relevant legislation, including the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) (EU) 2016/679;
- Comply with the principle T6, 'Data Governance' section of the [Code of Practice for Statistics](#), which states that: "Organisations should look after people's information securely and manage data in ways that are consistent with relevant legislation and service the public good." and
- Maintain the security and confidentiality of the data we receive, store, process and disseminate.

Arrangements for Maintaining Confidentiality of Statistical Data

As standard practice, we will ensure that all information is kept secure and ensure that information released does not reveal the identity of an individual or organisation or any private information relating to them taking into account information that might be available from other sources. These data cannot be forwarded to third parties without their prior agreement.

As a branch within the Department of Finance, we are required to comply with the [DoF Data Protection Policy](#). The [NISRA Privacy Notice](#) explains how NISRA will manage personal data collected and processed for statistics and research purposes.

Physical Security

WSA is located within People and Organisational Development's headquarters at Bruce Street, Belfast. The building has security staff that monitor/control access to the building and electronic swipe cards are used to restrict and control which offices staff can enter. Visitors must register at the building's reception and then must be accompanied by a staff member for the duration of their visit. The offices are monitored by CCTV and have an externally monitored alarm system in operation outside office hours. A clear desk policy is in place with all paper records securely locked in cabinets at night or when staff are not at their desks. The keys are then stored in secure key cabinets for each work area/branch within People & Organisational Development.

Working from home is an extension of the work place. Therefore all staff have a legal duty to protect personal information when not working in the office.

Technical Security

Access to the various IT systems is through terminals located within the secure Bruce Street site or via Secure Remote Access when not working in Bruce Street. All WSA staff members have their own unique password which only allows them access to the systems that they have been authorised to use and for which they have received appropriate training. The WSA encrypted laptop computers have no disk/CD Rom access and cannot be connected to mobile devices or to memory sticks. They also have boot-up passwords to further restrict access. The WSA virtual computer server is part of the NIGOV network that is secured and managed by ITAssist.

Databases are held on a network drive which is only accessible to the relevant members of WSA staff (as determined by staff responsibility and work areas) or within the Department's secure record management system, again with restricted access. Network drive access is reviewed and updated on a regular basis. Personal or sensitive data are not removed from the network without the relevant Head of Branch approval.

Organisational Security

The WSA Information Asset Owner oversees and manages systems to protect and maintain data held by us, with the support of Information Technology professionals and relevant statistical staff who work with the data.

Personnel Security

All staff who work with data about individual persons receive appropriate security checks (Counter Terrorism Checks). All WSA staff have received training relating to their obligations under the Data Protection Act, UK General Data Protection Regulation (GDPR) and Information Security through e-learning training modules and they are required to repeat/refresh this training every few years. Statisticians have been made aware of the contents of the National Statistician's Guidance 'Confidentiality of Official Statistics'.

Statistical Disclosure Control

When reporting figures or tabular results derived from datasets that could potentially result in the identification of an individual or private information about them, we will adopt disclosure control methods as appropriate. In doing so, we consider three types of disclosure risk in relation to the data about individual persons, or the statistics derived from the data:

Identity: If a person or persons can be identified (by either the persons themselves or someone else) then there is an identity disclosure risk.

Attribute: If confidential information about a person or group of persons is revealed and can be attributed to the person, or each person in the group, then there is an attribute disclosure risk.

Residual: If outputs from the same source, or different sources/databases, can be combined to reveal information about a person or group of persons, then there is a residual disclosure risk.

For each of our statistical and data releases, we will assess the risk of disclosure based on the following:

- Level of aggregation of the data;
- Number of tables produced from each dataset;
- Likelihood of an identification attempt;
- Size of the population; and
- Consequences of disclosure.

To minimise the risk of disclosure and maximise the utility of the statistics in our statistical releases, WSA uses an appropriate combination of statistical disclosure control methodologies including table design, rounding, primary suppression, and secondary suppression. We may use software for rounding and suppression purposes where feasible. Each of our statistical publications will provide details of the statistical disclosure control method adopted in the publication. Decisions on the type and extent of disclosure control to be applied will be taken by the statistician responsible for the relevant work area. These methods are adopted and applied in line with best practice guidance from Government Analysis Function (GSS) which can be found at the [Guidance Hub](#).

WSA Email Distribution List

Persons named on the WSA email distribution list (i.e. personal email addresses) will be informed how their confidentiality will be protected.

Information Assurance

Information Assurance is the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. The Department of Finance within the Northern Ireland Civil Service has a series of information assurance standards which provide detailed guidance on specific information assurance controls and practices. These must be adhered to in order to provide the assurance that information assets are protected and that WSA's information systems are operated and secured in a consistent manner and in compliance with national standards.

Sharing Data with a Third Party

As WSA is a data processor for some customers, all data shared with us is governed by Data/Information Sharing Agreements/Memoranda of Understanding, based on set templates. It has been agreed with the data owners that these data cannot be forwarded to third parties without their prior agreement.

Any transfer of personal/sensitive data (once a data sharing agreement is in place) will only take place in compliance with the Department of Finance's Information Assurance guidance to ensure that all such data transfers are conducted by secure means.

Requests for Information

All requests for information will be dealt with in a timely manner. All requests will be treated fairly and without prejudice, taking into account the public interest, the requirements of the Data Protection Act (1998), the UK General Data Protection Regulation (UK GDPR) 2016/679 and Freedom of Information Act (2000). Guidance on the Data Protection and Freedom of Information Acts can be found at the [Information Commissioners website](#).

Requests for information may be made to workforcestatisticsandanalysis@finance-ni.gov.uk or under the Freedom of Information Act may be made through the central Freedom of Information team at

foi@finance-ni.gov.uk or

Transparency and Open Government
Communications and Engagement Division
Department of Finance
2nd Floor West
Clare House
303 Airport Road
Belfast
BT3 9ED

While requests under FOI are treated on a case-by-case basis, the presumption is that requests for individual statistical records will be rejected. The legislation contains exemptions and processes that protect confidential information.

A copy of the Department's Notification to the Information Commissioner can be found at the [Information Commissioners website](#), search for "Register of Data Controllers".

Feedback

We welcome feedback from users on our Data Governance and Confidentiality Statement. Please send any comments to workforcestatisticsandanalysis@finance-ni.gov.uk.