
GLOBAL DRUG SURVEY LIMITED
Registered Office: Fergusson House, Level 5 124/128 City Road London EC1V 2NJ
www.globaldrugsurvey.com

**Global Drug Survey Information Security Policy**

**Issue Date: June 2016**
**Document Number: POL_4**
**Prepared by: CEO**

| | | |
|---|---|---|
| **Document Number: POL_4** | **Issue Date: June 2016** | **Version Number: 2.0** |
| **Status: Approved** | **Next Review Date: March 2019** | **Page 1 of 7** |

# Table of Contents

**Document purpose**
The purpose of this document is to provide guidance to all GDS partners, including out academic collaborators and corporate partners, on Information Security.

## 1.0 Introduction and background to GDS

Global Drug Survey (GDS) is an independent research organisation with information processing as a fundamental part of its purpose. It is important, therefore, that the organisation has a clear and relevant Information Security Policy, allowing it to comply with information legislation and to ensure all persons working on GDS projects are aware of their responsibilities.

GDS uses its data to create free harm reduction resources and apps. We also support the development of young researchers, produce academic peer reviewed publications and create data based reports for government, public health and corporate organizations.

GDS does not take funding from tobacco or alcohol industries.

## 1.1 GDS Methods and Mission

### 1.1.1 GDS Mission

Our mission is to make drug use safer regardless of the legal status of the drug. All our research is approved by university research ethics committees. All our data is anonymous. In our annual GDS surveys IP addresses are not collected and we record no personal details that allow identification of living persons in our linked data bases*

*All information is anonymous. A subset of participants (approximately 20%) provide their e-mail address which are stored in a separate encrypted stored database and consent to take part in future GDS projects. In such cases, anonymous data can be linked to e-mail addresses only after dual de-encryption and linkage by the Chief Technical Officer (CTO).

### 1.1.2 GDS Methods

GDS uses encrypted web surveys to gather data on drug use trends to inform public policy. Our data supports individuals and communities to adopt safer strategies regarding the consumption of psychoactive substances including alcohol. Anonymity, data security and confidentiality are central to everything we do.

### 1.2 GDS Surveys

We collect no personally identifiable data. E-mail address when they are voluntarily submitted as part of the annual survey are stored in a separate unlinked encrypted database.

### 1.3 Drinks Meter

E-mail address are not required for completion of the Drinks Meter and are only requested (but not stored) if individuals wish to receive an e-mail copy of their unique identifier which is provide to all those who complete the Drinks Meter.

## 2.0 Aims of this policy

The purpose of this document is to provide guidance to all GDS partners, including out academic collaborators and corporate partners, on Information Security. The purpose of GDS's Information Security Policy is to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology including the behaviour of the people who manage information as part of their work on GDS projects.

### 2.1 Preservation and protection

The aim of the GDS Information Security Policy is to preserve:

| | |
|---|---|
| Confidentiality | Access to Data shall be confined to those with appropriate authority. |
| Integrity | Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification. |
| Availability | Information shall be available and delivered to the right person, at the time when it is needed. |

## 2.2 Use of Technology

Information security is primarily about people but is facilitated by the appropriate use of technology, which is central to the operation of GDS.

The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and appropriate manner
- Assurance that GDS is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of persons working on GDS projects.
- A strengthened position in the event of any legal action that may be taken against GDS (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified and appropriate controls are implemented and documented.

# 3.0 Objectives

## 3.1 Security and confidentiality

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by GDS by:

- Ensuring that all persons working on GDS projects are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies.
- Working with other partners to develop collaborative approaches, systems and processes relating to information security.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to information security
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

# 4.0 Scope

## 4.1 Personnel within the Scope of this Document

Personnel associated with GDS are within the scope of this document:

- Core Research Team
- Senior Academic Mentor Group
- International Academic Partner Network
- Staff working on behalf of GDS when involved in GDS linked projects.

# 5.0 Roles and Responsibilities

## 5.1 Chief Executive

Information Security is everyone's business although responsibility resides ultimately with the Chief Executive but this responsibility is discharged through the designated roles of Senior Information Risk Owner (SIRO).

## 5.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for information risk within GDS and advises the Advisory Board, the Core Research Team and International Academic Network on the effectiveness of information risk management across the Organisation. They will also be responsible for:

- Ensuring that all persons working on GDS projects are aware of the information security policies, procedures and user obligations applicable to their area of work.
- Ensuring that all persons working on GDS projects are aware of their personal responsibilities for information security.
- Determining the level of access to be granted to specific individuals.
- Ensuring staff have appropriate training to ensure information security policies are complied with.
- Ensuring staff know how to access advice on information security matters
- Manage and implement this policy and related procedures.
- Monitor potential and actual security breaches.
- Ensure they receive immediate notification of any information security breaches

## 5.3 All persons working on GDS projects

All persons working on GDS projects are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in legal action and or dismissal from their current and all future GDS projects. In persons working on GDS projects should understand:

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- All staff are required to read the Information Governance Policy.
- How to report a suspected beach of information security within the organisation.
- Their responsibility for raising any information security concerns with the SIRO.

#### 5.3.2 External contractors

Data sharing agreements with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

# 6.0 Access Controls

## 6.1 Access to information

Shall be restricted to users who have an authorised business need to access the information and as approved by the CEO.

## 6.2 Computer Access Controls

Access to ICT facilities shall be restricted to authorised users who have business need to use the facilities.

## 6.3 Application Access Controls

Access to databases shall be controlled and restricted to those authorised users who have a legitimate business need e.g. CEO. Chief Bio-statistician and Core Research Team. Sharing any data outside the Core GDS group requires the GDS data sharing agreement to be signed

## 6.4 Equipment Security

To minimise loss of, or damage to, all assets, equipment shall be; identified, registered and physically protected from threats and environmental hazards.

## 6.5 Information Security

Events and Weaknesses: All GDS information security events, near misses, and suspected weaknesses are to be reported to the SIRO for investigation and fixing.

## 6.6 Data sharing (and storage) requirements

GDS data security and sharing requirements for Global Drug Survey Data

GDS data security and sharing requirements

All those working on GDS projects involving access to GDS, including Drinks Meter data agree to:

- Store the data on a secured server and keep no copies on non-encrypted computers or external hard devices and laptops
- Not share access to the data with any other person (except nominated research team members) who will comply with the same data storage requirements)
- Only conduct analysis related to the research topic specified below
- Create and share code/syntax to produce the results of the analysis with GDS for future replication if required
- Delete the data file on completion of the project, or as agreed through your ethics committee process
- Seek permission from Adam Winstock before commencing any work for publication or public presentation
- Submit drafts of related journal articles and/or conference presentations to Adam Winstock and/or other members of the GDS Core Research Team (Jason Ferris, Monica Barratt, Larissa Maier) for comment and opportunity for contribution and co-authorship
- If this work is being conducted as part of a funded project please disclose the nature of this funding to Adam Winstock
- You agree not to supply any versions of the output of this work to any third party without written permission from GDS
- Should you be requested to provide reports based on GDS data you direct the groups to us. No money can be made from GDS data reports to third parties without prior approval from GDS

**Drinks Meter**

- For Area Health Services and other health care organisation who use bespoke versions of the Drinks Meter local reports using anonymous pooled data is provided. Your organization's data will never be shared with another organization but pooled anonymised data may be used in research projects using composite date from all participants around the world using the Drinks Meter apps. GDS will provide your area with the raw data that we use to prepare your reports in the form of an excel file for your own analysis. This will include basic demographics, AUDIT scores, number of drinking days, units drank per day and per week, % drinking more than lower risk drinking guidelines and interest in reducing drinking and seeing help.

## 6.7 Business Continuity and Disaster Recovery Plans

GDS will implement a business continuity management system to ensure funding and technological services are in place to meet all the requirement of contract agreements.

## 6.8 Impact Analysis

Impact Analysis will be undertaken in all areas of the organisation.

Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

## 6.9 Disaster recovery plans

The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

# 7.0 Distribution and Implementation

This document will be made available to all persons working on GDS projects via direct e-mail.
A global notice will be sent to all persons working on GDS projects notifying them of the release of this document.

# 8. Monitoring

## 8.1: Compliance

Compliance with the policies and procedures laid down in this document will be monitored via the SIRO together with independent reviews by both Internal and External Audit on a periodic basis.

## 8.2: Revision and updating

The CEO is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

Note: As part of its development this document and its impact on equality has been analysed and no detriment identified.

## 9.0 Associated Documents

9.1 The following documents will provide additional information.

| REF NO | DOC REFERENCE NUMBER | TITLE |
|---|---|---|
| P01 | V2 | Information Governance Policy |
| P02 | V2 | Data Protection Policy |
| P03 | V2 | Confidentiality Policy |
| P05 | V2 | Data sharing policy and agreement |
| SER_1 | V1 | Drinks Meter Server Compliance Document |