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

www.globaldrugsurvey.com

Global Drug Survey Data Confidentiality Policy

Issue Date: June 2016
Document Number: POL_3
Prepared by: CEO

Document Number: POL_3	Issue Date: June 2016	Version Number: 2.0
Status: Approved	Next Review Date: March 2019	Page 1 of 6

Table of contents

Document Purpose

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all persons who work on GDS projects', sensitive business information or GDS data. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving 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 Confidentiality 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

1.1a. 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).

1.1b. 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 and objectives

2.1 All persons who work on GDS projects are bound by a legal duty of confidence to protect sensitive business information or GDS data they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the U.K. Data Protection Act 1998.

2.2 This policy sets out the requirements placed on persons who work on GDS projects when sharing information within GDS and between GDS and non GDS partner organisations.

2.3 Information can relate to GDS data, research projects, business contracts and app development, however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, mobile phones, digital cameras or even heard by word of mouth.

3.0 Scope

3.1 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.

4.0. Roles and Responsibilities

4.1 The Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that GDS policies comply with all legal, statutory and good practice guidance requirements. GDS is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

4.2 All other persons working on GDS projects

Confidentiality is an obligation for all persons working on GDS projects. The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all persons who work on GDS projects sensitive business information or GDS data. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

- Any breach of confidentiality, inappropriate use of GDS data, systems or knowledge of business sensitive/confidential information, or abuse of IT systems is a disciplinary offence, which could result in termination of access to GDS data and removal form current projects.

5.0 Principles

5.1 General principles

All persons working on GDS projects must ensure that the following principles are adhered to

- All data related to GDS projects must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access GDS data or other confidential information must be on a need-to-know basis.
- Disclosure of GDS data confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with the CEO directly.

5.2 GDS only collected anonymous data.

- Raw unit record data is not reported on.
- Data is unidentifiable.

5.3 Disclosing GDS data

- To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have sanctioned access to said data either following signing the GDS Data Sharing Agreement or following written permission form the CEO.
- GDS data can be disclosed:
    - As part of GDS approved research projects when appropriate ethical approval has been received (if required) and when the GDS Data Sharing Agreement has been signed
    - Only when it has been pooled
    - Linked databases to encrypted e-mails can only be released with written permission for the CEO and when appropriate ethical approval has been received (if required) and when the GDS Data Sharing Agreement has been signed.

- When there is explicit awareness for the purposes for the what the data will be used for
- That no funding from either the tobacco or alcohol industries have been used in the funding of the data request.
- When a named member of the Core Research Team has been identified to monitor data compliance and output from the project.
- Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, and faxes.

6.0 Transfer of information (see Data Security Policy)

- Care must be taken in transferring information to ensure that the method used is as secure as it can be. Encrypted cloud service transfer is the most reliable method. In most instances a Data Sharing/Information Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements see Policy 5
- Transferring patient information by email to anyone outside approved persons working on named GDS projects may only be undertaken by using encryption and with written permission from the CEO.

6.1 Persons working on GDS projects

May be held personally liable for a breach of confidence and must not:

- Leave any confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents, and
- Leave a computer terminal logged on to a system where GDS data or other confidential information can be accessed, unattended.

6.2 Passwords

Must be kept secure and must not be disclosed to unauthorised persons.

- Person working on GDS projects must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access.

7.0 Monitoring

7.1 Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance Steering Group.

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

7. 3 Equality Impact Assessment: As part of its development this document and its impact on equality has been analysed and no detriment identified.

8. Associated Documents

8.1 The following documents will provide additional information.

REF NO	DOC REFERENCE NUMBER	TITLE
P01	V2	Information Governance Policy
P02	V2	Data Security Policy
P04	V2	Information Security Policy
P05	V2	Data sharing agreement
SER_1	V1	Drinks Meter Server Compliance Document

Issue Date: June 2016
Document Number: POL_3
Prepared by: CEO