GLOBAL DRUG SURVEY

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

www.globaldrugsurvey.com

Global Drug Survey Data Security Policy

Issue Date: June 2016
Document Number: POL_2
Prepared by: CEO

Document Number: POL_2	Issue Date: June 2016	Version Number: 2.0
Status: Approved	Next Review Date: March 2019	Page 1 of 8

Table of Contents

Table of Contents 1
1.0 Introduction and background to GDS 2
1.1 GDS Methods and Mission 2
1.1.1 GDS Mission 2
Document purpose 2
1.1.2 GDS Methods 3
1.2 GDS Surveys 3
1.3 Drinks Meter 3
2.0 Data Protection Principles 3
2.1 Compliance 3
3.0 Scope 5
3.1 Personnel within the Scope of this Document 5
4.0 Roles and Responsibilities 6
4.1 Chief Executive 6
4.2 Senior Information Risk Owner (SIRO) 6
4.3 GDS partner responsibilities 6
5.0 Transfer of information 6
5.1 Data storage: 7
5.2 Personal Liability 7
5.3 Passwords 7
6.0 Distribution and Implementation 7
7.0 Monitoring 7
7.1 Compliance 7
7.2 Revision 8
8.0 Associated Documents 8

Document purpose

The purpose of this document is to provide guidance to all GDS partners, including our academic collaborators and corporate partners, on Data 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 Governance 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 Data Protection Principles

The lawful and proper treatment of data collected by GDS is extremely important to the success of our business and in order to maintain the confidence of the people who participate in our surveys, use our free resources and use our data report and consulting service. We ensure that the way GDS treats data submitted to our projects is done so lawfully, correctly and with full consent. GDS complies with requirements and principles of the UK Data Protection Act 1998

2.1 Compliance

GDS fully supports and complies, where required* with the eight principles of the Act which are summarised below:

1. Survey and app data shall be processed in accordance with the participant information sheet and requirements set out by the university research committees that approve our research (fairly and lawfully).
2. Survey and app data shall be obtained/processed for specific lawful purposes.
3. Survey and app data held must be adequate, relevant and not excessive (irrelevant to the work of GDS)
4. Survey and app data must be accurate and kept up to date.
5. Survey and app data shall not be kept for longer than necessary.

6. Survey and app data shall be processed in accordance with rights of the subject

7. Survey and app data must be kept secure.

8. Survey and app data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection.

*GDS has substituted 'personal data' for 'survey and app data' since we not collect names, addresses or dates of birth and all data is submitted anonymously. GDS is fully compliant with the Act, but we also wish to be act in the spirit of the act even though we do not collect personally identifiable data.

2.2 Information covered by the Act

Section 2 of the Data Protection Act 1998 defines sensitive personal information as information related to:

- o Racial or ethnic* origin;
- o Political opinions**;
- o Religious or other similar beliefs;
- o Membership of trade unions;
- o Physical or mental health or condition*;
- o Sexual life**; and.
- o Convictions, proceedings and criminal acts**.

* may be collected as part of the annual GDS and the Drinks Meter

** may be collected as part of the annual GDS only

Note: The Act's definition of "personal data" covers any data that can be used to identify a living individual. *Anonymised or aggregated data* is not regulated by the Act, providing the anonymization or aggregation has not been done in a reversible way. The data collected is completely anonymous, unless the participant chooses to share their contact details in order to be conducted regarding future research opportunities. In such instances the contact details are stored in a separate, unlinked, encrypted database, with access restricted to two members of the research team alone. The encryption keys are kept in a safe held by the CTO. No e-mails submitted to GDS or any other personal data is ever shared with any third parties.

2.3 GDS Surveys and Drinks Meter App

As part of both the annual GDS survey and the Drinks Meter app, GDS does collect personal information from people who choose to participate in our projects or utilise our free anonymous self-assessment tools. Such details support the provision of granular, personally meaningful feedback and to allow the drafting of high quality research papers. To this end all our research received university research ethics approval.

The information does not include name, address nor exact date of birth (month and day are collected by a minority of participants as part of unique IDs to allow trends among returning participants to be analysed); current age is also collected). Anonymous data is however collected on a range of sensitive issues including drug use, drug purchase, mental health, well-being and cultural background as well as age, gender, sexual orientation and broad geographical location details (country and in some cases, region and or city). No matter how it is collected, recorded and used (e.g. on a computer or other digital device) media, this personal information is dealt with properly to ensure compliance with the UK Data Protection Act 1998 (the Act).

2.3.1 GDS Surveys

We collect no personally identifiable data. Where an E-mail address is voluntarily provided in order to contact participants for follow up research the data stored on a separate unlinked encrypted database.

Data security and protection are taken very seriously. Reports, publications and other public communique of GDS data never involve unit record data: the reporting of analysis is based on pooled data. Both the GDS website and Survey Gizmo are encrypted. The risk of discovery through participation in the survey is extremely low, as participants' IP addresses are not collected, the data collection utilises web encryption, and the databases used to archive the data collected are also encrypted. The data collected is completely anonymous, unless the participant chooses to share their e-mails in order to be conducted regarding future research opportunities; in which cases the contact details are stored in a separate, unlinked, encrypted database, with access restricted to two members of the research team alone. The encryption keys are kept in a safe. No e-mails submitted to GDS or any other personal data is ever shared with any third parties. As the risk of social stigma would result from discovery of an individual's drug use by society at large, this risk is also highly unlikely, given the steps GDS is taking to limit any such discovery. These risks and the steps GDS has taken to mitigate them are shared with all potential participants in the participant information sheet which precedes the survey. To date, since 2012, we have never had any concerns raised by either participants or partnering organisations.

2.3.2 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.

The Drinks Meter and website are hosted on an encrypted website and data stored on a secure cloud servers which comply with best industry standards. No personally identifiable data is collected as part of the 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. So, although some aspects of data defined within the act is collected it is anonymised and cannot be connected to a living person.

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 Chief Executive

Overall accountability for procedural documents across the organisation as they relate to data security and corporate lies with the CEO. As the Accountable Officer they have overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting all statutory requirements and adhering to guidance issued in respect of information governance and procedural documents

4.2 Senior Information Risk Owner (SIRO)

This role will:

- Provide guidance on the responsibilities for all those persons who handle GDS data and ensure access to further guidance and support
- Provide clear lines of reporting and supervision for compliance with data protection and handling
- Carry out regular checks to monitor and assess new data handling including analyses of research data
- Ensure that ICT security levels meet industry standards
- Ensure the maintenance of all firewalls and secure access servers are in place at all times and;

  computer and data storage devices comply with data security requirements
- Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis.

4.3 GDS partner responsibilities

All partners within the GDS network who have access to the survey development site, survey data or app data will, through appropriate training and responsible management:

- Sign the data sharing agreement
- Observe all forms of guidance, codes of practice and procedures about the collection and use of survey and app data outlined in the data sharing agreement.
- Understand fully the purposes for which GDS uses the data only for the purpose that it has provided.
- Ensure the information is destroyed (in accordance with the provisions of the Act or research ethics committee requirements) when it is no longer required.

5.0 Transfer of information

- 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.

- *Data files, provided to researchers, are made available via CloudStor (A product of aarnet https://support.aarnet.edu.au/hc/en-us).

- *CloudStor encrypts all data in transit via TLS tunnels between the client and the ha-proxy off-loaders within the CloudStor environment. This includes data sent via the web browser, owncloud client and webdav.

5.1 Data storage:

- Electronic data files (and backups) are saved on a secure, password protected University server.

5.2 Personal Liability

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.

5.3 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 GDS data this constitutes a disciplinary offence.

6.0 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.

7.0 Monitoring

7.1 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.

7.2 Revision

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.

8.0 Associated Documents

8.1 The following documents will provide additional information.

REF NO	DOC REFERENCE NUMBER	TITLE
P01	V2	Information Governance Policy
P03	V2	Confidentiality Policy
P04	V2	Information Security Policy
P05	V2	Data sharing policy and agreement
SER_1	V1	Drinks Meter Server Compliance Document

Issue Date: June 2016
Document Number: POL_2
Prepared by: CEO