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 Information Governance Policy

Issue Date: June 2016
Document Number: POL_1
Prepared by: CEO

Document Number: POL_1	Issue Date: June 2016	Version Number: 2.0
Status: Approved	Next Review Date: March 2018	Page 1 of 8

Table of Contents

Document purpose

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

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. We do 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 and objectives of this policy

The purpose of this document is to provide guidance to all GDS partners, including our academic collaborators and corporate partners, on Information Governance. Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern research environment. It provides a consistent way for people working with GDS to understand a range of information handling requirements including:

- Information Governance Management.

- Confidentiality and Data Protection assurance.

- Corporate Information assurance.

- Information Security assurance. and

- Data sharing and secondary use assurance

2.1 Aims of this document

To maximise the value of our organisational assets by ensuring that data is:

- Held securely and confidentially.

- Obtained fairly and with full consent.

- Recorded accurately and reliably.

- Used effectively and ethically, and

- Shared and disclosed only as part of GDS approved projects.

2.2 Protection

To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental GDS will ensure:

- Information will be protected against unauthorised access.

- Confidentiality and anonymity of information will be assured.

- Integrity of information will be maintained.

- Information will be supported by the highest quality data analyses.

- Regulatory and legislative requirements will be met.

- Business continuity plans will be produced, maintained and tested.

- Information security requirements training will be available to all persons working on GDS projects, and

- All breaches of information security, actual or suspected, will be reported to, and investigated by the SIRO.

2.3 Governance Policy Framework

- GDS has developed a framework for its Information Governance (IG) Policy. This is supported by a set of Information Governance policies and related procedures to cover all aspects of Information Governance which are aligned with the activities of GDS

- The Key Information Governance Policies are:

Policies	
Information Governance Policy (P01)	The purpose of this document is to provide guidance to all GDS partners, including out academic collaborators and corporate partners, on Information Governance.
Data Security Policy (P02)	This policy sets out the roles and responsibilities for compliance with the Data Protection Act.
Confidentiality Policy (P03)	This policy lays down the principles that must be observed by all who work on GDS projects and have access to confidential business information and research data. All staff must be aware of their responsibilities for safeguarding confidentiality and preserving information security in order to comply with common law obligations of confidentiality
Information Security Policy (P04)	This policy is to protect, to a consistently high standard, all information assets. The policy defines security measures applied through technology and encompasses the expected behaviour of those who manage information within the organisation
Data Sharing Policy (P05)	The policy will ensure that all information held or processed by GDS is made available subject to appropriate protection of confidentiality and in line with the terms and conditions under which the data has been shared with GDS.
Drinks Meter Server Compliance Document (SER_1)	The purpose of this document is to provide detail on the compliance supported by our Drinks Meter server provider

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
- Persons 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)

The CEO of GDS is also the nominated SIRO (Senior Information Risk Officer). This role will be supported by the Chief Technical Officer (CTO) and will

- Take overall ownership of the organisation's Information Security Policy.

- Understand how the strategic business goals of GDS may be impacted by information risks, and how those risks may be managed.

- Advise corporate and academic partners on the effectiveness of information risk management across GDS

- Ensure any parties with whom data is shared sign the GDS data sharing agreement and understand their responsibilities

- Ensure data is not shared for any research project that requires ethical approval without the appropriate documentation being made available.

- Know what information comprises a dataset or is associated with projects and understands the nature and justification of information flows from GDS to any other party.

- Ensure that app data (Drinks Meter) is only provided to approved recipients and as part of pre-approved contract negotiations for the purposes outlined in the contract.

- The formulation and implementation of ICT related policies and the creation of supporting procedures, and ensuring these are embedded within the service, developing, implementing and managing robust ICT security arrangements in line with best industry practice;

- Effective management and security of GDS ICT resources, for example, infrastructure and equipment;

- Developing and implementing a robust IT Disaster Recovery Plan;

- Ensuring that ICT security levels required by industry standards are met;

- Ensuring 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 Information Governance Steering Group

- CEO (SIRO)
- Chief Technical Officer
- Chief bio-statistician
- Members of the GDS Core Research Team

4.4 Steering Groups Responsibilities

- Providing advice and guidance on internal Information Governance to all persons working on GDS projects.

- Monitoring outputs from data sharing agreements to ensure there is consistency of IG across the organisation.

- Developing and reviewing internal IG policies and procedures.

- Developing IG awareness for persons working on GDS projects.

- Ensuring compliance with Data Protection, Information Security and other information related legislation.

5.0 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.

6.0. Monitoring

6.1 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.

6.2 Revisions and updates

The CEO is responsible for the monitoring, revision and updating of this document on a 2-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.

7.0 Associated Documents

The following documents will provide additional information.

REF NO	DOC REFERENCE NUMBER	TITLE
P02	V2	Data Protection 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_1
Prepared by: CEO

Document Number: POL_1	Issue Date: June 2016	Version Number: 2.0
Status: Approved	Next Review Date: March 2018	Page 7 of 7