

Policy

Information Governance Policy

REFERENCE

IG 01

VERSION

1.0

APPLIES TO

All staff

APPROVED BY

Alfie Ruffell, Director

ORGANISATION

**VYBRAH LTD, trading
as SPEAK**

1.0 Executive Summary

- 1.1** This Information Governance (IG) Policy has been written to define the scope of Information Governance within SPEAK, to clarify its ever increasing significance with regards to controlled use and security of information - in particular person identifiable information - and to provide practical guidance to staff on how to ensure compliance with both legal obligations in this arena but also guidelines and best practice as laid down by the Information Commissioner's Office (ICO) and applicable UK data protection law.

2.0 Introduction

2.1 Information is a vital asset, both in terms of the delivery of services to SPEAK's clients and the efficient management of services and resources.

2.2 IG is formed by those elements of law and policy from which applicable information governance standards are derived. It encompasses legal requirements, central guidance and best practice in information handling, including:

ICO Data Sharing Code of Practice 2022

ISO 27001 Information Security Standard

Common Law of Confidentiality

UK GDPR / Data Protection Act (DPA) 2018

Data (Use and Access) Act 2025

2.3 IG plays a key part in supporting SPEAK's governance, service planning and performance management. It gives assurance to SPEAK and to individuals that personal information is dealt with legally, securely, efficiently, effectively and confidentially, in order to deliver a trustworthy, safe service to SPEAK's clients.

2.4 It is of paramount importance that information is effectively managed with appropriate policies and procedures in place to ensure this. It is also essential to have identifiable management accountability in order to provide a robust information governance framework to support the organisation.

2.5 SPEAK's IG Policy sets out a proportionate approach to information governance appropriate to SPEAK's size and the special category (health-related) data it processes. It is organised under the following headings, consistent with good practice for organisations handling sensitive personal data. It is summarised under four headings:

Openness

Legal compliance

Information Security

Quality assurance

2.6 Whilst a key focus of information governance is the use of information about clients and staff, it applies to information and information processing in its broadest sense and underpins both service delivery and corporate governance. Accordingly, it should be afforded appropriate priority.

2.7 The four fundamental aims of Information Governance are:

To support the provision of high quality support by promoting the effective and appropriate use of information.

To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.

To develop support arrangements and provide staff with appropriate tools and support to discharge their responsibilities to consistently high standards.

To enable organisations to understand their own performance.

3.0 Purpose

3.1 The purpose of this policy is to provide employees of SPEAK with a simple framework through which elements of IG can be met.

4.0 Duties and Responsibilities

- 4.1 It is the responsibility of all staff to familiarize themselves with this policy and all related Information Governance policies and documentation where applicable.
- 4.2 Staff must ensure at all times that high standards of data quality, data protection, integrity, confidentiality and records management are met in compliance with relevant legislation and regulatory guidance (ICO).
- 4.3 All managers and team leads must promote high standards of Information Governance.
- 4.4 Compliance with standards of IG is the responsibility of the Information Governance (IG) Manager, Chris Fox, who is also SPEAK's named Data Protection Officer (DPO) and operational IG lead. Overall accountability for governance, and approval of this policy, sits with Alfie Ruffell, Director of VYBRAH LTD.
- 4.5 The IG Manager will make regular reports on IG activity to the Director at SPEAK's leadership check-ins. SPEAK does not operate a separate governance group or committee, given its current size.

5.0 Approval process

Key Area	Accountable	Operational lead	Approval
Information Governance	Alfie Ruffell, Director, VYBRAH LTD	Chris Fox, IG Manager and Data Protection Officer	Approved by the Director. No separate working group or committee at SPEAK's current size.

6.0 Policy Principles

- 6.1** SPEAK supports the principles of corporate governance and recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. SPEAK has implemented security arrangements to safeguard both personal information about clients and staff and commercially sensitive information. SPEAK also recognises the need to share information about clients with relevant external agencies in a controlled manner consistent with the interests of the client and, in some circumstances, the public interest and SPEAK's Information Sharing Policy.
- 6.2** SPEAK believes that accurate, timely and relevant information is essential to deliver a high-quality, trustworthy service and to actively use information in decision-making processes. This is essential, not only to deliver a high-quality service but also to support sound decision-making and reporting to the organisations SPEAK works with. As such, it is the responsibility of all managers and team leads to ensure and promote high quality information and to actively use information in decision-making processes.
- 6.3** The IG Policy is divided into four parts: Openness; Legal Compliance; Information Security; Quality Assurance.

7.0 Openness

- 7.1 Non-confidential information regarding SPEAK and its services should be available to clients and the public through a variety of media. (The Freedom of Information Act applies only to public authorities, so this is a voluntary transparency commitment rather than a statutory duty for SPEAK.)
- 7.2 SPEAK will maintain clear records management practice appropriate to its size and the data it holds.
- 7.3 Clients should have ready access to information relating to the support SPEAK has provided them, and their rights over their own data.
- 7.4 SPEAK will have clear procedures and arrangements for liaison with the press and broadcasting media.
- 7.5 SPEAK will have clear procedures and arrangements for handling queries from clients and the general public.

8.0 Legal Compliance

- 8.1 SPEAK regards all identifiable personal information relating to clients and staff as confidential, except where national policy on accountability and openness requires otherwise.
- 8.2 SPEAK will establish and maintain policies to ensure compliance with the UK GDPR and Data Protection Act 2018, Data (Use and Access) Act 2025, The Human Rights Act 1998 and common law of confidentiality; Equality Act 2010.
- 8.3 As a requirement of the UK GDPR SPEAK has appointed a Data Protection Officer (DPO) to ensure personal data it holds is processed in compliance with all applicable data protection rules.
- 8.4 SPEAK will establish and maintain policies for the controlled and appropriate sharing of client information with other agencies, taking account of relevant legislation (e.g. The Crime and Disorder Act 1998, The Protection of Children Act 1999 (relevant to safeguarding referrals)).

9.0 Information and Cyber Security

- 9.1 This includes the implementation of the Data Protection Act 2018 and the Information Governance Standards, Information Security arrangements as detailed in ISO 27001. It has a high level of overlap with robust standards for management of records, (e.g. records, which are not stored correctly, may also be insecure) and with Quality Assurance, (e.g. accurate data is necessary to ensure high standards for Information quality).
- 9.2 SPEAK will establish and maintain policies to ensure the implementation of the Data Protection Act 2018, the Computer Misuse Act 1990, and any further applicable legislation and regulatory guidance for effective and secure management and processing of its information, its information assets and resources.
- 9.3 SPEAK's Incident Reporting system will be used to report, monitor and investigate all breaches of confidentiality and security. Where they meet the statutory threshold, breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours, in line with UK GDPR.
- 9.4 SPEAK will promote effective confidentiality, data protection and security practice to staff through policies, procedures and training.
- 9.5 SPEAK will establish and maintain protocols for the controlled and appropriate sharing of client information with other agencies, taking account of relevant legislation (e.g. Crime and Disorder Act 1998, Protection of Children Act 1990 (relevant to safeguarding referrals)). SPEAK is also committed to achieving the Information Security Standard ISO27001 and ISO/IEC 42001:2023, Artificial Intelligence Management System (AIMS) standard.

10.0 Information Quality Assurance

- 10.1** This includes the implementation of information quality standards for electronic and manual client information.
- 10.2** SPEAK will establish and maintain policies for information quality assurance and the effective management of records.
- 10.3** SPEAK will maintain rigorous data quality validation checks of data flows against national standards.
- 10.4** Managers will be expected to take ownership of, and seek to improve, the quality of data within their services.
- 10.5** Wherever possible, information quality will be assured at the point of collection.
- 10.6** SPEAK will promote data quality through policies, procedures and training.
- 10.7** IG policies should be reviewed and updated at least every two years.

11.0 Governance and Accountability

11.1 IG management across SPEAK is led by Alfie Ruffell, Director of VYBRAH LTD, who holds overall accountability, supported by Chris Fox as IG Manager and Data Protection Officer.

11.2 The responsibilities of the Director and the IG Manager include (but are not limited to):

developing, implementing and monitoring Information Governance practice appropriate to SPEAK's size and risk profile.

assigning roles, monitoring information incidents and authorising company-wide information processes.

co-ordinating and monitoring the IG Strategy across SPEAK.

11.3 The IG Manager will provide regular reports on all aspects of compliance to the Director.

12.0 Implementation

12.1 The Director is responsible for approving IG policies and work programmes, on the advice of the IG Manager. The IG Manager reports on all aspects of the agenda outlined above, and the Director and IG Manager keep this policy under review.

12.2 SPEAK will conduct an annual internal review of its information governance practice, using this policy and relevant ICO guidance as the benchmark, and build any resulting action plan from that review.

12.3 The implementation of policies in this area will be carried out across SPEAK by all involved staff and led by the IG Manager with support from SPEAK's leadership team. Training and awareness sessions appropriate to staff groups will be provided, widening existing training as new policies and initiatives are introduced.

13.0 Risk

- 13.1** SPEAK must ensure that it operates within a robust IG framework to reduce the risk of both potential litigation and compromise to the support SPEAK provides, in line with SPEAK's approach to risk management. Risk assessments will be carried out in the individual component areas as required by this policy.
- 13.2** SPEAK's Director, supported by the IG Manager, will oversee the development of information risk policy and strategy, take ownership of risk assessment process for information risk, review and agree action in respect of identified information risks, provide a focal point for the resolution of information risk issues, and ensure the Leadership Team is adequately briefed in information risk issues.

14.0 Training, Training Needs and Awareness

14.1 Annual IG Training and Cyber Security Training are mandatory for all SPEAK staff and contractors to ensure that SPEAK has sufficient capability to implement effective IG and Cyber Security systems and processes.

14.2 Training needs assessments will be carried out as appropriate for the individual component areas for specific staff groups.

14.3 SPEAK will adopt a structured approach to IG training and provide a comprehensive programme of IG training to all staff. Training programmes will aim to skill staff in all the key areas of IG and include:

compulsory induction training to all new staff as part of the formal induction programme;

group training sessions given either by SPEAK's IG Manager or specialist external trainers commissioned on their behalf;

National IG and Cyber Security e-learning modules.

14.4 To protect the wellbeing of clients and staff, SPEAK addresses the training needs of its mandatory and statutory training through a simple training needs assessment and a training log maintained by the IG Manager, appropriate to SPEAK's size.

14.5 Duties within this area are as follows:

Role	Responsibility
Director	Responsible for ensuring all staff and contractors are adequately trained for their duties, and for following up refresher training needs.
IG Manager	Maintains the training log, provides access to IG and cyber security training, and monitors and reports on completion.
Staff and contractors	To attend all relevant training as detailed in their induction and annual development review.

15.0 Administration and Monitoring Compliance

- 15.1** An assessment of compliance with requirements, of this policy will be undertaken each year. Annual reports and proposed action/development plans will be reviewed with SPEAK's leadership.
- 15.2** As part of SPEAK's annual review, audits will be undertaken or commissioned in all areas of IG as needed and fed back to SPEAK's leadership.
- 15.3** It is the responsibility of the IG Manager to ensure all procedural documents include the review/monitoring of all the minimum requirements set out in this policy.

Monitoring arrangements for compliance and effectiveness i.e. audit, review, etc.

Responsibilities for conducting the monitoring/audit.

Methodology to be used for monitoring performance measurement and audit.

Frequency of monitoring/audit, i.e. quarterly, on a rolling basis, etc.

Process for reviewing results and ensuring improvements in performance occur.

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements	Acting on recommendations and Lead(s)
All sections of this policy	IG Manager	Annual internal IG review	Reviewed and reported annually	Important issues reported to the Director and fed into the next revision of the policy.	IG Manager and Director

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements	Acting on recommendations and Lead(s)

- 15.4** Preparation, review, distribution of this document is the IG Manager's responsibility.
- 15.5** It is the responsibility of the IG Manager to monitor the procedures contained within the Policy on a regular basis, in order to ensure that all staff are adhering to them.
- 15.6** In the event of a suspected breach of these procedures, SPEAK reserves the right to initiate further measures, such as disciplinary procedures.

16.0 References

16.1 Acts of Parliament and other external guidance relevant to this policy includes:

Human Rights Act 1998
Computer Misuse Act 1990
Crime and Disorder Act 1998
Electronic Communications Act 2000
Regulation of Investigatory Powers Act 2000
Children Act 2004
Information Security Management - ISO 27001
Gender Recognition Act 2004
Civil Partnership Act 2004
UK GDPR / Data Protection Act 2018
Data (Use and Access) Act 2025
Cyber Security and Resilience Bill 2025