Information Governance Framework (IG)

Status of document: Approved
Version: 4
Date of approval: 30 January 2024
Effective from: February 2024
Owner: Senior Information Risk Owner
Author: Information Governance Officer
Planned next review date: February 2027

Contents

1. Policy Statement

1.1 We are committed to ensuring that our Information Governance (IG) is effective, considers privacy by design, and enables us to be transparent, responsible, and forward-thinking.

1.2 We have a statutory duty under the Opticians Act 1989 ("the Act") to process personal information to enable us to fulfil our statutory functions, including our duty to disclose, share and publish personal information when it is in the public interest to do so. We do this with careful consideration of our information responsibilities, under Data Protection legislation, the Human Rights Act 1998, and the Freedom of Information Act 2000 (FOIA), to ensure that our use of personal data is lawful, and properly controlled and that an individual's rights are respected.

1.3 In order to complete our statutory duties effectively, we collect and use information about the people with whom we work. We also collect third-party information when completing our statutory duties. The people – known as 'Data subjects' – include, but are not limited to, our employees, members, and workers, registrants, members of the public, stakeholders, contractors, and suppliers.

1.4 We understand our responsibilities as a data controller, registered with the Information Commissioner's Office, as a fundamental obligation in our role as a regulator and public body.

1.5 This IG framework contains five policies that must be adhered to by all employees, members, workers, contractors, and those who work on behalf of the GOC (collectively referred to as GOC's data processors). The framework and associated policies are supplemented with local departmental guidance for further detail regarding specific operational expectations.

2. Purpose

2.1 This framework and associated policies are a central point of reference for our approach to good Information Governance. The framework is intended to help employees, members, workers, contractors, and those working on our behalf to quickly locate the appropriate policy they require.

3. Scope and Framework Overview

3.1 This policy applies to all employees, members, workers, contractors, and those working on our behalf (either temporarily or permanently) are expected to act in accordance with this framework and associated policies.

3.2 Compliance with this policy is mandatory. Non-compliance for employees may be considered a disciplinary matter. Non-compliance for members is a breach of the terms of appointment and could result in a code of conduct investigation.

3.3 This framework and associated policies apply to all data that the GOC acquires, holds or processes – including personal, special category and confidential data.

3.4 This data can be held in any form or format, including electronic or hardcopy, and includes databases, spreadsheets, reports, medical records, diaries, emails, CCTV, audio recordings, paper files and handwritten notes.

3.5 Non-personal information must also be appropriately managed and protected, and many of the principles in this policy are applicable to non-personal information and must be applied accordingly.

3.6 The IG framework is composed of five policies:

- **Data Protection Policy** - outlines our approach to complying with the UK GDPR and DPA 2018 and other data regulations, including our roles and responsibilities, our compliance with the seven DPA principles, and handling requests for personal data (SARs);
- **Freedom of Information Policy** - outlines our approach to managing our Freedom of Information (FOI) duties, including our publications scheme, and responding to FOI requests.
- **Disclosure Policy** - outlines our approach to disclosing personal information and our approach to publishing information;
- **Data Sharing Agreement Policy** - outlines our conditions on sharing information with third parties. This includes the template that is used for our DSAs; and
- **Data Retention Schedule Policy** – outlines our approach to retaining, storing, and maintaining information.

3.7 The framework and policies are supplemented with individualised department induction briefings on data breaches and Information Governance.

3.8 Our Information Technology policy details our approach to IT security and fair usage of all electronic devices. (Information Technology Policy)

4. Glossary of Terms

Confidentiality	Data which is provided 'in confidence'
Data	For the purpose of this document, the terms data, and information are synonymous.
Data breach	A breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Data controller	Responsible for determining the purpose and use of the data it holds, processes, and transfers.

Data processor	All of our employees, members, workers, contractors, and those who process data on our behalf are data processors. They are personally responsible for handling information in line with the relevant data protection legislation and with our operational policies and procedures.
Data Protection Act (DPA 2018)	The Data Protection Act 2018 and superseding legislation which set out a data subject's individual data protection and data privacy rights.
Data Protection Legislation	Includes (but is not limited to) any relevant and applicable data protection legislation, such as the UK General Data Protection Act and the Privacy and Electronic Communications Regulations which sits alongside the UK General Data Protection Act.
Data Sharing Agreement (DSA)	An agreement that sets out the purposes of sharing information.
Data subject	The person who is the subject of the personal information.
Destruction	The permanent destruction of information.
DPO	Data Protection Officer.
EIR	Environmental Information Regulations.
Freedom of Information (FOI)	The legislation within the Freedom of Information Act 2000 (FOIA) which gives people the right to request information from public authorities.
IAO	Information Asset Owner.
ICO	Information Commissioner's Office: the organisation that oversees compliance with data protection legislation, FOIA and other legislation.

Information	There are seven information categories referred to within this framework: confidential, personal, (sensitive) special category personal data, criminal offences, anonymous and pseudonymous. **Confidential information** – Confidential information means any non-public information pertaining to the GOC. **Personal data** – Personal data means any information which relates to an identified or identifiable natural person ("data subject"). An identifiable person is one who can be identified, directly or indirectly, in particular by a reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. **(Sensitive) Special category personal data –** (Sensitive) special category personal data are personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership, data concerning health or sex life and sexual orientation; genetic data or biometric data. **Data relating to criminal offences –** data relating to criminal offences may only be processed by national authorities. National law may provide derogations, subject to suitable safeguards. Comprehensive registers of criminal offences may only be kept by the responsible national authority. Within this policy, this information is referred to as **special category personal data** however there are different specific conditions for processing this data. **Anonymous data –** data which, even when combined with other information from different agencies, does not identify an individual, either directly or by summation. **Pseudonymous data –** Pseudonymous data are still treated as personal data because they enable the identification of individuals (albeit via a key). If the "key" enables the re-identification of individuals it should be treated as personal data. An individual may consider certain information about themselves to be particularly private and may request other data items to be kept confidential e.g., any use of pseudonym where the true identity needs to be withheld to protect them.

Information Governance (IG)	The specification of decision rights and an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving, and deletion of information.
Information Security Incident	An umbrella term to describe a data breach or a near miss.
Non-Disclosure agreement (NDA)	A legally binding contract establishes a confidential relationship when handling information.
Near miss	An unplanned incident where personal information was put at risk of unauthorised access, loss, or corruption, but does not constitute a data breach.
Privacy Impact Assessment	An assessment to help identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy.
Public Interest	Within information governance, this is generally considered something which serves the interest of the public.
Senior Information Risk Owner (SIRO)	Is a professional who has responsibility for implementing and managing information risks within the organisation.
Subject Access Request (SAR)	A request for personal information under current legislation laws.

5. Compliance

5.1 This section outlines the compliance required within all of the policies which form part of the IG Framework.

5.2 All employees, members, workers, contractors and those working on our behalf are responsible for acting in compliance with the legislation and the principles and procedures detailed in the policies within this framework and associated local Information Governance processes.

5.3 Managers are responsible for monitoring the compliance of their teams on a regular basis and for addressing any non-compliance. Compliance will be verified through various methods including, but not limited to, periodic compliance checks, and internal and external audits. Senior Management Team (SMT) is responsible for monitoring compliance with the policies alongside the Audit, Risk and Finance Committee (ARC). Reporting arrangements are set out in the section 'transparency' below.

5.4 Failure to comply with the legislation and this framework and/or associated policies may result in disciplinary action, and failure to comply may also result in individual prosecution.

5.5 Any exceptions to this framework and associated policies must be approved by the Senior Information Risk Owner in advance.

5.6 Actual, suspected, or potential breaches must be immediately reported by the person who has discovered the incident ('the reporter') must read and comply with the below:

- All employees, members, workers, contractors, and those working on our behalf are expected to immediately report actual, suspected, or potential breaches of information security.

- This must be reported within 24 hours of becoming aware of the breach, the reporter must submit a security incident report form and send it to the Information Governance Officer, their line manager and their department's director. Failure to report within this timescale may be considered a disciplinary offence.

- This is important because if the breach is a high risk, it may need to be reported to the ICO within 72 hours of the moment when someone first becomes aware (this can be the reporter, third party, etc.) of the breach.

- The Information Governance Officer will need to complete an investigation into the incident. If the incident is serious, conducting a full investigation in accordance with our Investigation Policy may be considered.

- Any manager who is made aware of the breach as per this policy is expected to make all attempts to minimise the impact, in collaboration with the Information Governance Officer.

- The Information Governance Officer will ensure that the following stages of breach management are completed promptly, please use our internal breach management process when reporting a breach. (Data Breach Process).

- The incident will then be reported to the senior management team, who will discuss the outcome and actions.

- All incident reports will be signed off by the Data Protection Officer (DPO) once an investigation has been completed, who will then decide if the breach needs to be reported to the ICO.

- Remedial and permanent measures to mitigate the risk of reoccurrence will be implemented by the appropriate department(s) and will be supported by the Information Governance Officer.

- The Information Governance Officer will record all actions taken and lessons learned from the incident or near miss and will ensure these are periodically distributed within the organisation for continued learning and awareness.

5.7 If any person alters, defaces, blocks, erases, destroys, or conceals any record held by a public authority with the intention of preventing the disclosure of information to an applicant who has made a Freedom of Information request or Subject Access Request, they will be guilty of an offence.

6. Reasonable Adjustments

6.1 Should you require any reasonable adjustments to use or comply with this group of policies, please contact the EDI Manager or People and Culture (P&C) (for employees) to further discuss your requirements:

Phone:	020 7580 3898 (switchboard)
Email:	edi@optical.org
Post:	EDI Manager / P&C General Optical Council 10 Old Bailey London, EC4M 7NG

6.2 Should a member of the public require assistance to put their request in writing, they should be referred to the P&C Team, who will make all reasonable attempts to support them.

6.3 Information will be provided in the requested format, where possible. Special consideration will be given to those requesting information in a more accessible form (for example, large print or Braille).

7. Transparency

7.1 The IG framework and associated policies will be published on our website. We will report compliance with our IG framework and policies to SMT and ARC every quarter. Information may also be included in our annual reports or performance reports.

7.2 We will store all information related to these processes securely and in line with our Retention Schedule, ensuring secure destruction when appropriate.

7.3 We will regularly review our Information Asset Register in line with our Data Retention policy to ensure we have the appropriate security mechanisms in place for the data we process.