Data Protection Policy

Our data protection policy outlines our approach to complying with current data legislation and other data regulations, including our roles and responsibilities, our compliance with data protection principles, and handling requests for information.

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 recognise the importance of effectively managing how we use and store information to ensure we adhere to current data legislation.

2. Purpose

2.1 This data protection policy sets out our commitment to:

- comply with current Data Protection Legislation;
- protect the rights of our employees;
- being open and transparent about how we store and process information;
- help mitigate the risks of a data breach; and
- provide tools and resources that support good Information Governance practice.

3. Scope

3.1 This policy applies to:

- Employees (whether permanent or temporary) and workers;
- members; and
- contractors working with, or on behalf of, the GOC.

3.2 Compliance with this policy is mandatory. Non-compliance for employees may be considered a disciplinary matter.

3.3 If you require further advice and guidance, you should contact the Information Governance Team at IG@optical.org.

4. Roles and Responsibilities

4.1 The General Optical Council is the Data Controller (ICO registration - Z5718812) and is responsible for determining the purpose of the data that is collected and how it is processed.

4.2 As part of our commitment to ensuring that due attention is paid to your responsibilities, we have a number of Information Governance (IG) roles to help us ensure compliance with the legislation. They are:

Senior Information Risk Owner (SIRO) - Director of Change

- Accountable to the Council for appropriate and effective information risk management.
- Responsible for and takes ownership of our IG policies and acts as an advocate for IG risks.
- Ensures that an effective information assurance governance structure is in place, including information asset ownership, reporting, defined roles, and responsibilities.
- Ensures that there is a systematic and planned approach to the management and quality assurance of our records.

Data Protection Officer (DPO) - Head of Governance

- Has operational responsibility for data protection within the GOC.
- Informs and advises the organisation and its employees about their obligations to comply with data legislation.
- Provides technical advice and guidance on matters relating to IG.
- Monitors compliance with data protection laws, including managing internal data protection activities, advising on data protection impact assessments (Impact Assessment Screening Tool), training employees, members, workers, and contractors and conducting internal audits.
- Liaises with the Information Commissioner's office (ICO) when required, and with other regulatory bodies on data protection policy development.
- Supported by the Information Governance Officer who deputises in their absence.

Information Governance Officer (IGO)

- Manages all GDPR processes in accordance with GOC policies and procedures within the relevant timeframes.
- Identifies training needs across the organisation and provide this to the relevant departments.
- Updates policies and procedures to ensure these are fit for purpose.
- Manages all data breach incidents and supports departments in mitigating risks.
- Is the organisation's first point of contact for any information governance related queries.

Information Asset Owners - Heads of and those who directly report to Directors

- Accountable to the SIRO for assuring the security and use of their information assets.
- Identifies, understands, and addresses risk to the information assets that they "own".
- Responsible for managing the information that is produced, received, owned, and managed by their business area and ensures that this is in line with our policies.
- Continuously reviews and manages their risks.
- Reports any concerns to the SIRO bi-annually, or more frequently, if required.
- Ensures all employees within their department complete mandatory data e-learning learning and that they are aware of their responsibilities concerning personal data.
- Conducts or initiates privacy impact assessments (Impact Assessment Screening Tool), in line with the policy.

• Ensures all processes and contractors are documented, especially those in which high-risk data is processed.
Data Processors – All individuals who process data on GOCs behalf
• Personally responsible for handling the information securely • Must follow our policies and procedures • Must complete Information Governance training which is provided upon joining the GOC and throughout their employment.

5. Data Protection Act and UK GDPR

5.1 The Data Protection Act has two main aims:

- To protect individuals' fundamental rights and freedoms, notably privacy rights, in respect to processing personal data, and
- To enable organisations to process personal information in the course of legitimate business.

5.2 Data Protection legislation stipulates how we collect and process personal data lawfully in a way that is fair to the individuals that the information is about (the data subjects) and meets their reasonable expectations. Processing includes virtually anything thing that can be done to information, including acquisition, storage, and destruction.

5.3 As a data controller, we are responsible for and must be able to demonstrate, compliance with the seven Data Protection principles when processing personal data. These principles are set out in chapter 2 (35-40) of the Data Protection Act requires that personal information is handled as follows:

Principle 1 – It shall be processed lawfully, fairly, and in a transparent manner about individuals.
Principle 2 – It shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
Principle 3 – It shall be adequate, relevant, and limited to what is necessary for relation to the purposes for which they are processed.
Principle 4 – It shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased, or rectified without delay.
Principle 5 – It shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject

to the implementation of the appropriate technical and organisational measures required by the Data Protection Act to safeguard the rights and freedoms of individuals.

Principle 6 – It shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5.4 There is an additional principle, known as the 'accountability principle', which requires public bodies to take responsibility for what they do with personal data and how they comply with the other principles. As such we are required to have appropriate measure and records in place to be able to demonstrate our compliance with the law and our policies.

6. Information Management

6.1 We will ensure that privacy impact assessments (in our Impact Assessment Screening Tool) are completed as part of our procurement, policy review, and project management processes.

6.2 We will manage an Information Asset Register to ensure that information and privacy risks are appropriately managed.

6.3 We will ensure that our employees, members, workers and contractors are trained in data protection and information requests and that their knowledge is refreshed annually. We will also provide supplementary training and guidance to remind our employees and members of our operational expectations.

6.4 We will ensure that there are confidentiality provisions in the contracts of GOC employees, members and workers, including temporary employees or contractors, and similar instructions for those working on our behalf including solicitors, expert witnesses, and third-party suppliers.

6.5 Where no contracts are in place, we will ensure that Data Sharing Agreements are established with any third parties.

7. Lawful basis for processing and Privacy Statements

7.1 We are clear that different types of data we process are done so under a different lawful basis. This includes processing by:

- **Contract** – this applies to the employee, member, worker, contractor, and third-party processor data.
- **Legal obligation** – for all data subjects when we are required to process their personal data to conduct a legal obligation, such as financial checks or complying with a court order.
- **Public task** – for activity related to our four statutory functions, like education and registration of Optometrists, Dispensing Opticians and Optical Businesses, and fitness to practise investigations.

- **Legitimate interests** – for activity related to our general working, such as handling queries not related to our functions, corporate complaints, or conducting wider research.
- **Consent** – for our marketing and promotional activities, even when in the public interest (but not when the information relates to our public task). We keep an active register within our CRM system which informs us if individuals have given consent. Individuals will always have the right to withdraw their consent at any time by emailing IG@optical.org.

7.2 We are committed to being open and honest with individuals about how we intend to use their personal data. We ensure that data subjects are given a privacy notice at the time of collection. We make every attempt to ensure that our privacy notices are uncomplicated, in plain English (or Welsh upon request), and in a reasonably prominent position on any hardcopy form or electronic screen. All new privacy notices must be approved by the Data Protection Officer. We also use our privacy statement – published on our website – to go into further detail regarding our use of personal data.

7.3 If we make any changes to our privacy notices or statements, we will update data subjects using the most appropriate method.

8. Individual Rights

8.1 Every data subject has rights to how their information is handled. These are the rights:

- **to be informed** - the right to be informed about the collection and use of their personal data.
- **of access** - the right to access their data and supplementary information. the right of access allows individuals to be aware of and verify the lawfulness of the processing.
- **to rectification** – the right to have inaccurate personal data rectified or completed if it is incomplete.
- **to erasure** - the right to have personal data erased. The right is not absolute and only applies in certain circumstances.
- **to restrict processing** - the right to request the restriction or suppression of their data. The right is not absolute and only applies in certain circumstances.
- **to data portability** - the right to data portability allows individuals to obtain and reuse their data for their purposes across different services.
- **to object** - the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

- **about automated decision-making and profiling** - the right to be provided with information about the automated individual decision-making, including profiling.

8.2 The lawful basis of processing determines which individual rights can be invoked or requested. More information can be found on www.ico.org.uk.

8.3 All requests to invoke the above rights must be sent immediately to IG@optical.org so that the request can be processed, and further guidance may be offered to data subjects.

9. Subject Access Requests (SAR)

9.1 We will process Subject Access Requests (SAR) in line with the Data Protection Act, chapter 3 (45) right of access by the data subject.

9.2 Data subjects have the right, upon written request, to be informed:

- whether or not information about them is being processed by us,
- to be given a description of the information,
- the purpose of our processing and to whom it may be disclosed, and
- to be provided with the information we hold in an intelligible form.

9.3 Employees, members, contractors, and those working on our behalf must be trained to recognise requests for information as the request will not necessarily be labelled under the correct legislation and does not require to be specifically phrased as a SAR.

9.4 The Information Governance Officer manages SAR requests received, and all requests must be sent immediately to IG@optical.org as we must adhere to a response time of 1 calendar month from receipt of the request.

10. Information Accuracy

10.1 When collecting personal information, we will endeavour to ensure it is accurately recorded, especially when provided verbally. We will periodically request that data subjects review the data we hold about them to ensure it remains accurate.

10.2 We will help data subjects to update and correct their data (rectification), but we may require evidence or verification to make some changes for data protection purposes.

10.3 We will make every attempt to hold one single version of the information to avoid duplication and minimise the risk of data being inaccurate across versions.

10.4 If we receive information from a third party, we will endeavour to find out how accurate the information is, if there is any doubt of its accuracy, and when it was last verified.

11. Non-UK Information

11.1 We will always seek written consent from the data subject before sending any personal information outside of the UK. Individuals will always have the right to withdraw their consent at any time in writing to the GOC.

11.2 We consider Data Protection legislation and regulations during procurement and our decision-making.

12. Volume of Personal Data

12.1 We are committed to collecting and using only the minimum amount of personal data required for the purpose(s) specified.

12.2 Where de-personalised or anonymous information would suit our purposes, we will always aim to anonymise the information, to reduce the amount of personal data that we hold.

12.3 Each employee, member, worker, contractor, or person working on our behalf is responsible for managing their outlook mailbox and their personal space on the IT systems and is expected to regularly review and delete unnecessary emails or documents containing personal information. This includes the sent items, deleted items, and recycle bin.

The same principle must be applied for shared mailboxes, for which the owner will be identified in the Information Asset Register.

13. Information Archiving, Retention, and Disposal

13.1 We will adhere to our Retention Schedule to ensure that we are not holding personal information for longer than necessary.

13.2 When archiving information, Information Asset Owners are responsible for ensuring that they have an accurate record of the information that has been archived, and ensure any boxes of archived material are labelled appropriately, including:

- Information Asset Owners name and Department;
- Type of information;
- Box number; and
- Date for destruction.

13.3 When archiving, it is important to group documents by type and retention length, ensuring that one box only contains information of the same type and retention

length. Failure to do so will have implications for adherence to our Retention Schedule. Failure to implement may result in disciplinary proceedings.

13.4 When deleting main copies of data, as per the timelines set out in the Retention Schedule, a destruction log must be maintained by the Information Asset Owner. This should contain a list of the information destroyed, the date, and the method of destruction.

13.5 Paper documents containing personal information must be securely destroyed in the confidential shredding bins.

14. Information Security

14.1 We are committed to protecting all personal information, including in collection, storage, and transfer.

14.2 Personal information (including business sensitive information) must not be disclosed in any format, whether accidentally or not, to any unauthorised third party without the data subject's consent and without prior authorisation from the Data Protection Officer or delegated manager (such as Head of Case Progression or the Information Governance Officer). Data subjects will always have the right to withdraw their consent at any time in writing to the GOC.

14.3 For further information about standards of conduct expected from all employees, members, and third-party contractors working on our behalf, please refer to our Information Technology Policy.

15. Information Asset Register

15.1 The information asset register is defined as a centralised log of all information that is held by the GOC including but not limited to the nature of the data (i.e., personal or sensitive data), what information is held, and the physical location of the data.

15.2 An information asset can be defined as;

- An operating system
- Infrastructure
- Business application
- Records
- Information
- IT Hardware

It will have recognisable and manageable value, risk, content, and lifecycles and can range from a basic Excel spreadsheet or database, within the GOC there are many such systems, both electronic and paper that holds information relating to personal, sensitive, and commercially sensitive data.

The responsibility for the information asset register sits on many levels depending on the action that is needed. However, there will be an Information Asset Owner assigned from each department, whose responsibility is to ensure their departmental data is being maintained or destroyed appropriately.

15.3 The Asset Register must be reviewed and updated every three months by Information Asset Owners. It is the responsibility of each department to ensure that their Assets are up to date. The Senior Management Team will review the Information Asset Register every six months to ensure compliance.

Information Governance Officer

15.4 The governance and compliance team are responsible for the overall maintenance and monitoring of the register. It is their duty to ensure that each department conducts a six-monthly review/update on all areas of their register.

Key actions;

- Promoting information asset awareness throughout the GOC by organising training, and awareness and providing written procedures and guidance that are widely available to staff.
- Assisting with investigations into breaches of confidentiality or data loss of personal and sensitive information.
- Co-ordinate the notifications of such breaches with SMT and the Information Commissioners Office (ICO).
- Develop and maintain the Information Asset Register working with Information Asset Owners (IOAs).
- Working with the IOAs and IT to help mitigate risks to their information assets.

Senior Information Risk Owner (SIRO)

15.5 The Senior Information Risk Owner (SIRO) has overall accountability and responsibility for the Information Governance of the GOC and is required to provide assurance that all risks to the GOC, including those relating to information, are managed and mitigated effectively.

Head of Governance

15.6 It is up to the Head of Governance to ensure and act as an advocate for Information Governance including reporting any issues to the senior management team, which feeds into the leadership team in the GOC governance structure.

Key actions;

- Provide advice and support to the leadership and senior management team (SMT) on the annual governance risks in relation to the risk register.

- Liaise with the information asset owners (IOAs) on resolution and/or discussion of issues along with compliance.
- Ensure the GOC has a plan to monitor and achieve set requirements for Information governance, including the culture of the our activities and staff.
- Approve all information asset areas of the Business Continuity Plan with SMT.

Information Asset Owners (IOA)

15.7 IOAs are responsible for overseeing that the information within their departments is accurate and in compliance with data protection legislation.

Key actions;

- Lead and promote a culture of high standards of Information Governance
- Know what information is contained in the asset including any additional or removed information.
- Know who has access to the asset and why, including access levels if part of an electronic system.
- Ensure compliance with data-sharing agreements.
- Understand the risks to the asset and be able to provide assurance to the SIRO and SMT that data is secure in the event of a breach.
- Ensure that all new assets within their department are reported to Compliance for inclusion in the register along with a completed privacy impact assessment
- Any assets destroyed are recorded on the destruction register and follow the correct retention period with the retention policy.
- Ensure that procedures and controls are in place to ensure the integrity and availability of the information assets.
- Provide updates when required as part of the Compliance Monitoring Programme.

Information Asset Administrators (IAA) – Individual Staff

15.8 Information Asset Administrators (IAA) are usually the staff members who understand and are familiar with the assets in their area.

Key actions;

- To maintain the general data quality of their information asset and report any areas of concern to the IAO.
- Ensure that personal or commercially sensitive data is not unlawfully exploited.
- Recognise any potential or actual security incidents and report this to the IAO
- Under the direction of IAO, ensure any asset to be destroyed is done so securely when no longer required.
- Ensure appropriate access to information assets and report any issues that may occur.

15.9 All staff need to be aware that confidentiality and security of information include all information relating to members, employers, and third parties. All staff are expected to;

- Have read and complied with the GOCs data protection policies.
- Attend all mandatory training and awareness meetings.
- Ensure all information held is accurate, relevant, up-to-date, and used appropriately.
- Ensure that all personal identifiable data is kept secure and only shared when necessary.
- Ensure that all data breaches or near misses are reported to the Information Governance Officer.