Information governance handbook

About the handbook

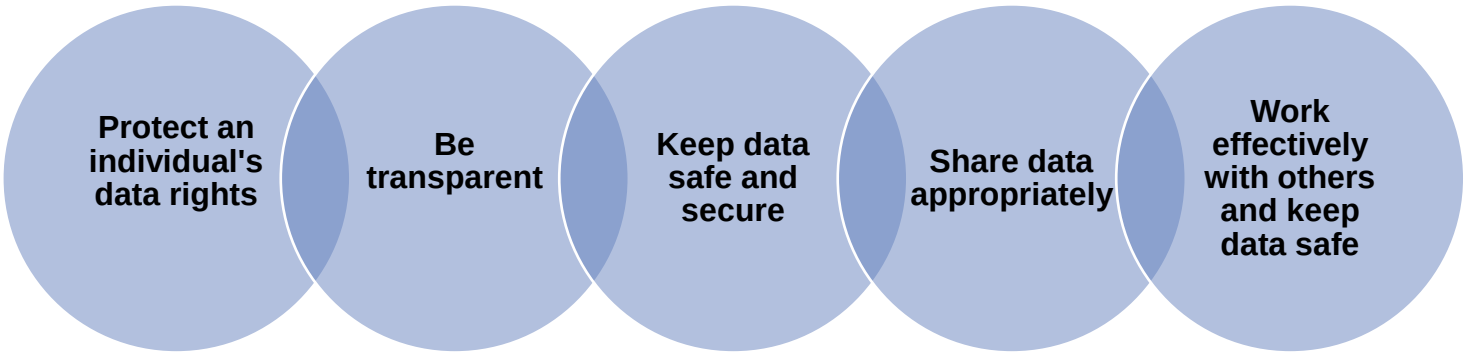
This handbook sets out our approach to Information Governance and applies to GOC employees, members and those working on our behalf.

Use this document as a central point of reference for all of the associated IG policies and standards expected.

Handbook Contents

Status of document:	Final (Framework and Handbook)	
Version:	3	
Approved by:	Council	
Date of approval:	July 2016	
Effective from:	October 2016	
Owner:	Head of Governance	
Author:	Compliance Manager	
Relevant legislation:	• Data Protection Act • Privacy and Electronic Communications Regulations 2003 • General Data Protection Regulations (GDPR) • Access to Medical Records Act 1988 • Human Rights Act 1998 • Freedom of Information Act 2000 • Opticians Act 1989 • The Common Law Duty of Confidence • The Recognition of Professional Qualifications Directive 2005/36 • Environmental Information Regulation 2004 • Computer Misuse Act 1990 • Access to Health Records Act 1990	
Linked policies:	• Data Sharing Agreement • IT policies • Acceptable Behaviour when communicating with the GOC	
Impact Assessment:	https://www.optical.org/en/news_publications/Publications/equality-and-diversity-reports.cfm	
Impact Assessment completion:	July 2016	
Impact Assessment review:	May 2020	
Next policy review date:	**May 2020**	
Location - Website:	https://www.optical.org/en/about_us/data-and-information/index.cfm	
Updates:	November 2017	Disclosure policy updated at Council, minor corrections throughout and re-branded
	March 2018	Policies updated to reflect GDPR and Data Protection Bill

Information Governance (IG) Framework



Contents

1. 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 (HRA) and the Freedom of Information Act 2000 (FOIA), to ensure that our use of personal data is lawful, 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 acquire information about others in the course of those dealings. The people – known as 'data subjects' – include, but are not limited to, our employees and members, 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 a number of policies which must be adhered to by all employees, members and those who work on behalf of the GOC (collectively referred to as GOC '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 about our approach to safe IG. The framework is intended to help employees, members and those working on our behalf to quickly locate the appropriate policy they require.

3. Scope and framework overview

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

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

3.3. 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.

3.4. 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.

3.5. The IG framework is composed of five policies:

3.5.1. Data Protection policy;

3.5.2. Freedom of Information policy;

3.5.3. Disclosure policy;

3.5.4. Information Security policy; and

3.5.5. Data Sharing Agreement policy (printed separately to Handbook).

IG Framework:

Data Protection policy - outlines our approach to complying with the DPA and other data regulations, including our roles and responsibilities, our compliance with the eight DPA principles and handling requests for personal data (SARs).

Freedom of Information (FOI) policy - outlines our approach to managing our Freedom of Information (FOI) duties, including our publications scheme and responding to FOI requests.

Information Security policy - outlines the key principles to ensuring that our information is kept securely, including office security; handling, transferring and sharing information; and how to report suspected or actual data breaches.

Disclosure policy - outlines our approach to disclosing personal information and our approach to publishing information.

Data Sharing Agreement (DSA) policy - outlines our conditions on sharing information with third parties where we do not have a contract in place. This includes the template that is used for our DSAs.
Note: This policy is part of the IG framework however it is **not** included in the IG Handbook because it is required in its entirety when used to establish DSAs with other parties

3.6. The framework and policies are supplemented with local departmental guidance and our IG Toolbox Talk briefings.

3.7. Our IT policy details our approach to IT security and fair usage of all electronic devices.

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, 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)	the Data Protection Act 1998 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 EU General Data Protection Regulations, the Data Protection Act 1998 and superseding legislation, Privacy and Electronic Communications Regulations
Data Sharing Agreement (DSA)	the specific agreement which 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 who oversees compliance with data protection legislation, EIR and FOIA
Information	There are six 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 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 a pseudonym where the true identity needs to be withheld to protect them.
IG	Information Governance
Information Security Incident	an umbrella term to describe a data breach or a near miss
IT	Information Technology
NDA	Non-disclosure agreement
Near miss	an unplanned incident where personal information was put at risk of authorised access, loss or corruption, but does not constitute a data breach
Partner, partnership organisation	any organisation which enters into agreement or works with the GOC
Privacy Impact Assessment (PIA)	a tool to help identify the most effective way to comply with our data protection obligations and meet individuals' expectation of privacy. Sometimes referred to as a DPIA (data protecting impact assessment)
Public interest	within IG, this is generally considered as something which serves the interest of the public
SIRO	Senior Information Risk Owner
Subject Access Request (SAR)	a request for personal information, under the DPA.

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 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 IG 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, internal and external audits.

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

5.5. Any exceptions to this framework and associated policies must be approved by the Compliance team in advance.

5.6. Actual, suspected or potential breaches must be immediately reported by the person who has discovered the incident ('the reporter') to their line manager and the Compliance team (or their respective line managers if unavailable), in accordance with the Security Information Reporting Process.

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 an FOI or SAR request, he or she is 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 Compliance Team, the Head of Governance, or HR (for employees) to further discuss your requirements:

6.1.1. phone: 020 7580 3898 (switchboard)

6.1.2. email: edi@optical.org

6.1.3. post: Compliance Team / Head of Governance / HR
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 Compliance 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 for 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.

7.2. We will report on compliance with our IG framework and policies to the Senior Management Team and the Audit and Risk Committee on a quarterly basis. Information may also be included in our annual reports or performance reports.

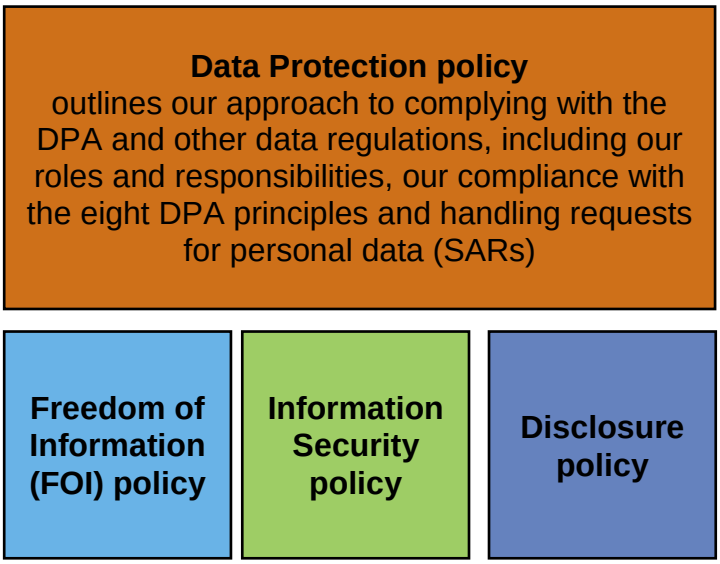
7.3. We will publish summaries of all FOI responses on our website, where we have disclosed information, for up to 18 months. The published responses will contain no personal information. Trends may also be considered to test the effectiveness of the Publications Scheme. This may include reviewing the process to agree information to be published.

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

8. Index of Topics and Policies

Topic	Policy
Archiving	Data Protection
Clear Desk, locked workstation	Information Security
Compliance	Information Governance Framework
Data breaches	Information Security
Data Protection Principles	Data Protection
Data Sharing Agreements	Data Sharing Agreement
Disclosing personal information	Data Protection; Disclosure
Disposal / Destruction	Data Protection
Email Security	Information Security
Equipment (laptops, mobile phones, iPads)	IT policy
FTP information disclosure	Disclosure
Freedom of Information (FOI) Request	Freedom of Information
Glossary	Information Governance Framework
ID badges	Information Security
Information Requests	Freedom of Information ; Data Protection
Office keys	Information Security
Office security	Information Security
On-line security	IT policy
Passwords	Information Security
Patient Records management	Local FTP process
Posting	Information Security
Printing	Information Security
Privacy Impact Assessments	Data Protection
Privacy Notices	Data Protection
Protective Marking	Information Security
Publication Scheme	Freedom of Information
Publishing information	Disclosure
Reasonable Adjustments	Information Governance Framework
Redaction	Disclosure
Removable Media	Data Protection; IT policy
Reporting data breaches	Information Security
Retention	Data Protection
Request for information (personal or business)	Freedom of Information ; Data Protection
Request to stop processing	Data Protection
Re-use of information	Freedom of Information
Roles and Responsibilities	Data Protection
Sharing (disclosing) data	Data Protection; Disclosure, Data Sharing Agreements
Subject Access Requests	Data Protection
Transparency	Information Governance Framework
Visitors	Information Security

Data Protection policy



Contents

1. Roles and responsibilities

1.1. We are a Data Controller (ICO registration - Z5718812) and are responsible for determining the purpose of data that is collected and the means by which it is processed.

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

Senior Information Risk Owner (SIRO) - Director of Resources
• **accountable to the Council for appropriate and effective information risk management** • responsible for and takes ownership of our IG policies and acts as 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 • providers 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, training employees and members, and conducting internal audits • liaises with the ICO when required, and with other regulatory bodies on data protection policy development; • supported by the Compliance team who deputise in their absence.
Information Asset Owners (IAOs) - Heads of and those who directly report to Directors
• **accountable to the SIRO for providing assurance on 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 ensure 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 protection e-learning and that they are aware of their responsibilities concerning personal data. • conducts or initiates privacy impact assessments, in line with the policy; · ensures all processes and contractors are documented, especially those in which high risk data is processed.
Data Processors - all GOC employees, members, and those who process data on our behalf
• **are personally responsible** for handling information in line with the data legislation and our operational policies and procedures.

2. Data Protection Act summary

2.1. Data Protection Act has two main aims:

2.1.1 to protect individuals' fundamental rights and freedoms, notably privacy rights, in respect of personal data processing; and

2.1.2 to enable organisations to process personal information in the course of legitimate business.

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

2.3. As a data controller, we are responsible for, and must be able to demonstrate, compliance with the following six Data Protection principles when processing of personal data. These principles (which are set out in Schedule 1 of the Act) require that personal information is handled as follows:

Principle 1 – It shall be processed lawfully, fairly and in a transparent manner in relation to 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 in 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 personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Principle 5 – It shall 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 implementation of the appropriate technical and organisational measures required by the Data Protection Act in order to safeguard the rights and freedoms of individuals; and

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 against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Information management

3.1. We will ensure that privacy impact assessments are completed as part of our procurement, policy review and project management processes.

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

3.3. We will ensure that our employees and members are trained in Data Protection and Information Requests and that their knowledge is refreshed annually. We will also provide supplementary training and guidance, including process notes to remind our employees and members of our operational expectations.

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

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

4. Lawful basis for processing and privacy notices

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

- 4.1.1. Contract – this applies to employee, member and third party processor data.
- 4.1.2. 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.
- 4.1.3. Public task – for activity related to our four statutory functions, like the education and registration of optometrists and dispensing opticians, and fitness to practise investigations.
- 4.1.4. Legitimate interests – for activity related to our general working, such as handling queries not related to our functions, corporate complaints, or conducting wider research.
- 4.1.5. Consent – for our marketing and promotional activities, even when in the public interest (but not when the information relates to our public task).

4.2. 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 and in a reasonably prominent position on any hardcopy form or electronic screen. All new privacy notices must be approved by the DPO. We also use our privacy statement –

published on our website – to go into further detail regarding our use of personal data.

4.3. If we intend to use personal data for another purpose to that which was set out in the privacy notice, and the data subject would not expect us to use it for that purpose, we will seek consent.

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

5. Individual rights

5.1. Every data subject has rights to how their information is handled. These are the right(s):

5.1.1. **to be informed** - the right to be informed about the collection and use of their personal data;

5.1.2. **of access** - the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing

5.1.3. **to rectification** – the right to have inaccurate personal data rectified, or completed if it is incomplete.

5.1.4. **to erasure** - the right to have personal data erased. The right is not absolute and only applies in certain circumstances.

5.1.5. **to restrict processing** - the right to request the restriction or suppression of their personal data. The right is not absolute and only applies in certain circumstances.

5.1.6. **to data portability** - the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

5.1.7. **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

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

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

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

6. Subject Access Requests (SAR)

6.1. We will process subject access requests (SAR) in line with the Data Protection Act.

6.2. 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.

6.3. Employees, members 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.

The Compliance team manages SAR requests received, and all requests must be sent immediately to foi@optical.org as we must respond to all requests within one month of receipt.

7. Information accuracy

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

7.2. 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.

7.3. 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.

7.4. 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.

8. Non-EEA information

8.1. We will always seek written consent from the data subject before sending any personal information outside of the EEA.

8.2. We consider Data Protection legislation and regulations during procurement and consider this within our decision-making.

9. Volume of personal data

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

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

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

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

10. Information archiving, retention and disposal

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

10.2. When archiving information, IAOs 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:
- 10.2.1. IAO's name and department;
- 10.2.2. type of information contained;
- 10.2.3. number of the box; and
- 10.2.4. date for destruction.

10.3. 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.

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

10.5. For paper documents containing personal information, these must be securely destroyed in the confidential shredding bins.

11. Information security

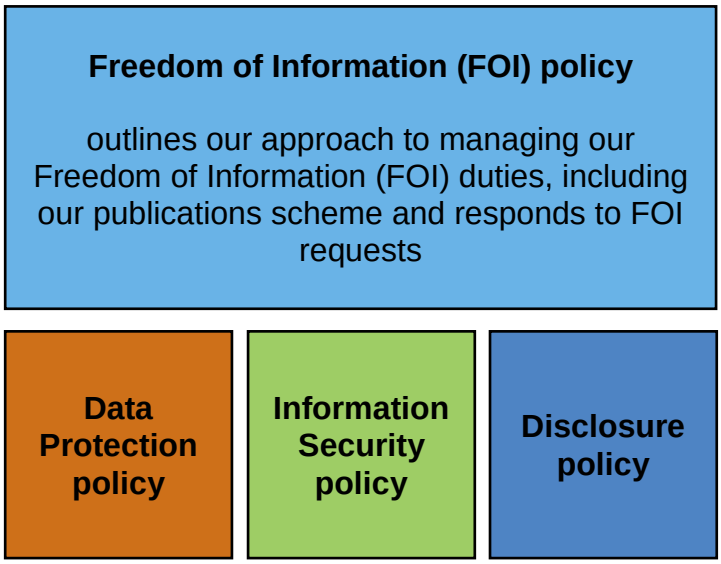
11.1. We are committed to protecting all personal information, including in collection, storage and transfer.

11.2. Access to personal information will be restricted to those who need to access it and have the right to access it.

11.3. Personal information must not be disclosed either orally or in writing, whether accidentally or not, to any unauthorised third party without the data subject's consent without prior authorisation from the DPO or delegated manager (such as Head of Case Progression or the Compliance team).

11.4. 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 security policy and our IT policy.

Freedom of Information (FOI) policy



1. Freedom of Information Act (FOIA) summary

1.1 The FOIA gives people the right to request information from public authorities. It is intended to promote a culture of transparency and accountability amongst public sector bodies and increase public understanding of how public authorities carry out their duties, why they make the decisions they do and how they spend public money.

1.2 All FOIA requests are considered alongside the following legislation:

1.2.1 Data Protection Act – which provides individuals with a right to access information about themselves; and

1.2.2 Environmental Information Regulations 2004 (EIRs) – which provides individuals with a right to access environmental information. They apply to information held by or on behalf of public bodies carrying out a public function.

1.3 All information we create or store is subject to the requirements of the FOIA provided that:

1.3.1 we retain possession of the information; or

1.3.2 we have provided the information to another public body; or

1.3.3 the information is held by a third party on our behalf.

Publication Scheme

1.4 Under FOIA, we are required to proactively publish information and it is a statutory duty to develop and maintain a publication scheme that has been approved by the ICO.

1.5 Our publication scheme demonstrates our commitment to make certain information publically available and explains how information can be obtained. The scheme also details if charges are applicable. Our publication scheme is published on our website and is reviewed periodically.

2. Right of access

2.1 The FOIA gives individuals and organisations the legal right to:

2.1.1 ask if a public authority is holding information; and if so

2.1.2 obtain access to the information held, within 20 working days from the day after receipt of the valid written request.

Valid Requests

2.2 Requests for information must be made in writing (paper or electronic) and must state the name and address (postal or email address) of the requester and state the information that they are requesting.

2.3 FOI requests must not be accepted verbally, although where a requester is unable to write their request, we will try to assist them.

2.4 There is no requirement for the requester to explain the reason for their request or to specify that it is a request being made under the FOIA.

3. Exemptions

3.1 Whilst we always look to respond to requests fully, requesters are not always entitled to be given all of the information they request.

3.2 Information released under FOI must be considered as being released into the public domain.

3.3 There are currently 23 exemptions from the right of access to information, which are set out in Part 2 of the FOIA.

3.4 In broad terms there are two types of exemptions:

- 3.4.1 Absolute exemptions – where the right to information is completely negated by the exemption; and
- 3.4.2 Qualified exemptions – where we identify a possible exemption, but must weigh up competing interests to decide whether it serves the interest of the public better to withhold or disclose the information. This is known as the public interest test.

3.5 Examples of absolute exemptions are:

- 3.5.1 Section 21 – Information reasonably accessible by other means
- 3.5.2 Section 40 – Personal information
- 3.5.3 Section 41 – Information provided in confidence
- 3.5.4 Section 44 – Information whose disclosure is prohibited by law

3.6 Examples of qualified exemptions (where the public interest test applies) are:

- 3.6.1 Section 22 – Information intended for future publication
- 3.6.2 Section 30 – Investigations and proceedings conducted by public authorities
- 3.6.3 Section 36 – Prejudice to effective conduct of public affairs
- 3.6.4 Section 43 – Commercial interests
- 3.6.5 Section 42 – Legal professional privilege

3.7 When deciding whether to apply a qualified exemption (and withhold information) valid consideration must be given to decide if releasing the information would serve the public interest and whether it would outweigh the reasons behind exemption.

3.8 The public interest factors must outweigh the interests protected by the exemption concern in order to be disclosed. It is not enough that there is merely a public interest attached to the information being requested.

3.9 The person making the request has an interest in the information but this does not constitute “public interest”.

3.10 If the requestor has had GOC access restrictions applied under our Acceptable Behaviour policy, we will consider each request on its merits but may alter the way we correspond regarding the request(s), in line with the restrictions.

4. Handling FOI requests

4.1 This section outlines our legal responsibilities when processing a request.

4.2 FOI requests are coordinated by the Compliance team, who will record all FOI/SAR requests and relevant correspondence in line with our Retention Schedule.

4.3 All employees, members and those working on our behalf are responsible for ensuring FOI requests are promptly forwarded to the FOI inbox (foi@optical.org) and to respond to requests from the Compliance team in a timely manner.

4.4 We will acknowledge all written FOI requests within five working days of the request being received.

4.5 The 20 working day timeline starts from the working day after receipt of the request and continues during working days including if the office is closed to the public. Bank holidays in UK territories are not considered as a working day, even if the offices are open.

4.6 Each request will be considered individually on its own merits.

4.7 Our duty is to confirm or deny whether the requested information is held and, if we hold the information, provide it in the requested format. If the requested information is not held, it would normally be reasonable to inform the requester. However, there may be exceptional cases where it would not be reasonable to confirm nor deny if the requested information is held.

4.8 In most circumstances, within 20 working days after the date of receipt, we will tell the requester whether the information is held and if the information is not considered exempt, we will provide it in the format required as soon as reasonably practical.

4.9 If an exemption is being considered, and we require additional time to complete a public interest test, we will promptly notify the requester of the exemptions that we are considering and provide a new deadline for response. We will not exceed a further 20 working days in order to consider the exemption.

4.10 In some cases, a request may be refused. If so, a refusal notice will be issued setting out the decision, the exemption relied on and the reasons why. If the exemption is a qualified one then the public interest test reasoning will also be explained.

4.11 Responses will always have contact details of the person who has handled the request, except in exceptional circumstances where SMT have agreed through the Acceptable Behaviour policy that this is not to be completed.

4.12 Responses will always set out the method of complaint if they are not satisfied with our response and explain their right to ask the ICO to decide whether the individual's request has been properly dealt with.

Fees

4.13 The FOIA provides for public authorities to either charge for or decline requests for information that would cost more than £450 to respond to. This is referred to as the 'appropriate limit'.

4.14 We are required to estimate whether a request is likely to breach the appropriate limit and, where appropriate, may charge a fee for complying with a request for information.

4.15 Any fee will be calculated in accordance with the FOIA regulations and the requester will be notified within 20 working days of the request being received. We are not required to comply with the request until the fee has been received in full.

4.16 We will respond to straightforward requests for information free of charge and will only charge when the costs breach the appropriate limit of £450.

5. FOI request appeals and complaints

Stage one: Internal review

5.1 If the requester is not happy with our response they can ask us, in writing and within 40 calendar days of the response, to complete an internal review. Their request should be addressed to the Compliance Team.

5.2 An employee with no prior involvement, usually of a higher grade, will reconsider their request and respond within the timescale.

5.3 Internal Review requests will be acknowledged within five working days of receipt and a response provided no later than 20 working days after receipt.

Stage two: Complain to ICO

5.4 Requesters that remain dissatisfied may complain to the ICO on any of the following grounds, failure to:

5.4.1 provide the information requested;
5.4.2 respond to the request within 20 working days;
5.4.3 explain why more than 20 working days was needed;
5.4.4 provide advice and assistance;
5.4.5 provide information in the requested format;
5.4.6 clearly explain any reason for refusing a request; or
5.4.7 correctly apply an exemption under the FOIA.

5.5 The ICO will decide whether the request has been handled appropriately in accordance with FOIA and will provide a decision notice, to both the requester and the GOC.

5.6 The ICO will not consider a complaint:
5.6.1 when the applicant has not exhausted our internal complaints procedure;
5.6.2 where there has been undue delay in making an application to the ICO;
5.6.3 where the application is frivolous or vexatious; or
5.6.4 where the application has been withdrawn or abandoned.

5.7 If the decision goes against us, the ICO will set out the actions that we are expected to take to correct the issues and by when.

Stage three: Information Tribunal

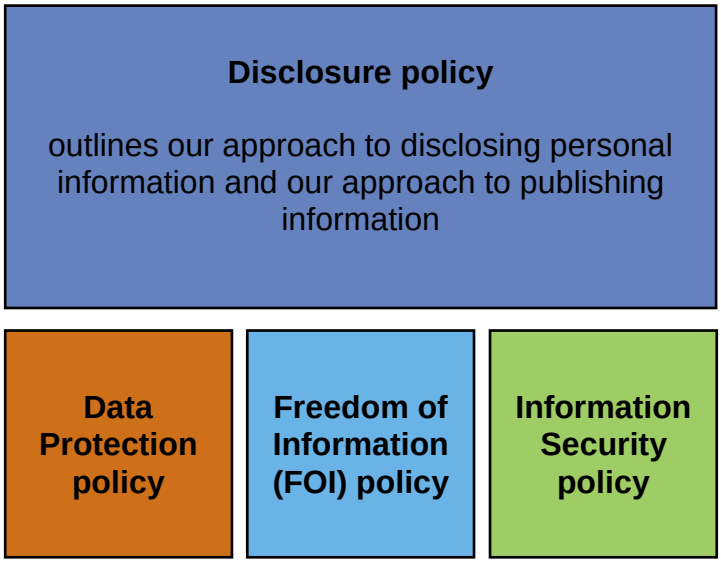
5.8 Either the applicant or the GOC can appeal against the ICO's decision notice to the independent Information Tribunal. Information regarding the right of appeal will be included in the ICO's decision notice.

6. Re-use of Public Sector Information regulations 2015 (RPSI)

6.1 Within the FOIA, the RPSI regulations 2015, allow for 're-use' of some public sector information for a purpose other than the initial public task it was produced for.

6.2 Should you wish to re-use any of our public information in this manner, please email the Compliance Team at FOI@optical.org, who will send you a form to complete, sign and return.

Disclosure policy



1. Our general approach to publication and disclosure

1.1 We seek to regulate in an open, transparent and proportionate manner – this applies to all of our statutory functions. This policy outlines our approach to routine publication and disclosure of our information.

1.2 We disclose information in accordance with our statutory disclosure duties as set out within the Optician's Act 1989 s. 13C(3) whereby:

'The Council may disclose to any person any information relating to –

a) A registered optometrist's or registered dispensing optician's fitness to practise;
b) A business registrant's fitness to carry on business as an optometrist or a dispensing optician, or to carry on both businesses; or
c) A student registrant's fitness to undertake training,

which they consider to be in the public interest to disclose.'

1.3 We are also subject to a range of other legislative duties such as (but not limited to) the Data Protection Act (DPA), Freedom of Information Act 2000 (FOIA), the Human Rights Act 1998, Public Interest Disclosure Act 1998 (PIDA) and the General Data Protection Regulations (GDPR).

1.4 In general, we consider something to be in the public interest if it may benefit the wider community. In assessing the public interest, we will consider all relevant factors, including the number of people affected, their age and/or vulnerability, any wider impact on health & safety, and the administration of justice. The public interest might also require us to make disclosure to the NHS, the Disclosure and Barring Services, the police, social services, other regulators and the Secretary of State for Health.

1.5 Disclosure under public interest applies to both personal and commercial information.

1.6 The publication of FTP information provides valuable information about standards expected of our registrants, helps to maintain public confidence in the professions we regulate and assists the public to make informed choices. However, publication must be proportionate and must take account of the interests of registrants and others involved in the process. For example, we do not routinely publish information about FTP investigations prior to FTP Committee stage.

Publication Scheme

1.7 We routinely publish and make available certain information – which is explained within our Publication Scheme.[1] For further information, please refer to our Freedom of Information policy.

[1] https://www.optical.org/download.cfm?docid=DC883928-BF92-4D48-9A7D14779F5531DB

Disclosure of GOC employees and members' names

1.8 We publish the names of senior management, members and some contractors working on our behalf. We may disclose the names of other employees if this is in the public interest.

1.9 We will not routinely publish any information about individual Case Examiners involved in a case, but we may disclose this in the public interest.

2. Information from other organisations

2.1 We do not normally disclose information about decisions by other statutory bodies or organisations, for example the Disclosure and Barring Services. Requests for this information should be directed to the responsible organisation.

3. Disclosure within the Fitness to Practise (FTP) process

3.1 This section outlines the routine disclosures we make as part of our FTP process. Any requests which fall outside of the below will be considered on a case by case basis and in accordance with this policy.

3.2 A FTP investigation includes the:

- 3.2.1 initial investigation by the Registrar (delegated to the Executive);
- 3.2.2 consideration of the allegation by the Case Examiners or Investigation Committee; and
- 3.2.3 consideration of the allegation by the FTP Committee (FTPC).

3.3 We have a statutory duty to notify the Secretary of State for Health that we have opened a FTP investigation[2]. In all other circumstances we apply this policy and make decisions in the public interest[3].

During an open investigation

3.4 We have a statutory duty[4] to notify the registrant that we have received an allegation of impaired FTP. We usually provide the registrant with a copy of the complaint form, redacted as appropriate.

3.5 There may be some circumstances where we outline the nature of the allegation rather than provide a copy of the complaint form, for example:

- 3.5.1 there is an ongoing investigation (NHS or police) which could be jeopardised should the allegation be disclosed;
- 3.5.2 disclosure could place a person at risk and we want to ensure there are safeguarding procedures in place;
- 3.5.3 the complainant has reason to have their identify kept confidential; and/or
- 3.5.4 disclosure would be inappropriate for other reasons, for example, where the case involves several registrants.

[2] s.13C(2)a Opticians Act 1989
[3] In line with s.13C(3) Opticians Act 1989 – power to disclose in the public interest.
[4] S. 13C(1) Opticians Act 1989

3.6 We will inform the complainant that we have opened an investigation and the name of the registrant(s) we have opened it against.

3.7 We have a statutory duty[5] to notify a registrant's employer of an investigation. If deemed appropriate, we usually provide limited information to:

3.7.1 those by whom a registrant is employed under a contract of employment; and

3.7.2 those by whom the registrant is engaged to provide services, including the provision of locum services.

3.8 We will also notify a registrant's employer(s) (using the definitions at 3.7 above) if the registrant is subject to an interim order by the FTPC.

3.9 If issues concerning the investigation are already in the public domain, we may decide in the public interest to confirm publicly that an investigation is continuing and/or the fact of an interim suspension or interim conditions order.

3.10 Where a complaint falls under the Public Interest Disclosure Act 1998, we will endeavour to comply with requests for someone's identity to remain confidential, for example through appropriate redaction, unless there is a public protection requirement to disclose or we are ordered by a court to disclose.

3.11 We may adopt the same approach with other witnesses, for example vulnerable witnesses or where we consider there to be a risk to the witness through disclosure of their name. It is important for all complainants and witnesses to note that it may be difficult to keep a complainant's identity confidential throughout the FTP process. It is important to note that it may be difficult to keep someone's identity confidential throughout the FTP process.

On conclusion of the investigation

3.12 Before an allegation is considered by the Case examiners / Investigation Committee / Registrar ("preliminary decision makers"), we will disclose to the registrant all documentation or information relevant to the allegation which we intend to place before the preliminary decision makers, in accordance with our Rules[6].

3.13 Upon receipt of the registrant's representations, (unless we consider it inappropriate) we will disclose these to the complainant and invite written representations. We will disclose the complainant's representations to the registrant but will not invite written representations unless we determine that this is required.

3.14 We will only place documents in front of the preliminary decision makers if they have been seen by the registrant - except for Rule 15 cases that do not proceed

---

[5] s.13C Opticians Act 1989

[6] Rule 5(3) – 'unless the registrar considers it inappropriate, the registrar must disclose to the maker of the allegation such representations as are received from the registrant, inviting written comments within a specified period'.

to a full review, where we will disclose to the registrant (by way of the full case examiners' decision) that an application has been made and rejected.

Outcomes of the Preliminary Decision Makers

3.15 We will notify the registrant, complainant, and employers of the outcome of the preliminary decision. We will inform other witnesses whether preliminary decision makers have closed the case or referred it for a FTPC hearing.

3.16 We will disclose the full preliminary decision only to the registrant, their legal representative and the complainant.

3.17 We will disclose warnings imposed by the preliminary decision makers only to the registrant and the complainant, not to employers or others.

3.18 We will not publish information on our website at any stage prior to consideration by the preliminary decision makers unless an interim order is imposed by the FTPC.

3.19 We may also notify others where this would be in the public interest.

Interim orders

3.20 Where it is necessary for the protection of the public, in the interests of the registrant or otherwise in the public interest, we may apply for an interim order (IO). This could mean that a registrant is placed under conditions or suspended while the substantive investigations are ongoing[7].

3.21 Interim order hearings are held in private. We do not publish notices of new interim order hearings, however we do publish notices of interim order hearing reviews. Where the Committee decides not to impose an interim order, we will not publish any information on our website or the register.

3.22 Where an interim order is imposed, a summary will be published on our website, redacted as appropriate. The order will also be recorded on our register.

3.23 We may disclose further information where this would be in the public interest.

Cross-disclosure

3.24 Some complaints lead to investigations into another registrant's practice. In these cases, we will consider what information to disclose to the other registrant.

3.25 We will inform the initial registrant of the proposal to share information, and invite representations. We will then consider these representations alongside the public interest and the interests of other registrant(s).

[7] s.13L(1) Opticians Act 1989

Health assessments

3.26 Medical reports prepared following a review of the registrant's medical records or a personal assessment will be disclosed to the preliminary decision makers, the FTPC and GOC employees with a defined business requirement (redacted as appropriate).

3.27 We will not disclose the registrant's medical records to any third party, unless there is a public interest in doing so. Access to medical records will be restricted to employees with a defined business requirement. We will ensure that medical records are stored securely in compliance with the DPA. Medical records will be returned to the original record holders by secure delivery (or, in the case of copy records, securely destroyed) once the matter, or any associated appeal is concluded.

Performance assessments

3.28 Performance assessors will observe the registrant in practice, usually observing their examination of four patients. We will not disclose to the patients that we are investigating the registrant.

3.29 The performance assessors' report and associated documents will be disclosed to the preliminary decision makers, the FTPC and GOC employees with a defined business requirement (redacted as appropriate).

The Fitness to Practise Committee (FTPC)

3.30 The majority of our FTPC hearings are held in public. Hearings for cases solely involving health are heard in private. Where information regarding a registrant's health is disclosed during any part of a public hearing, this information will be redacted from the determination before it is published.

3.31 Some cases involve more than one issue, for example conduct and health. In these cases, the FTPC will hear as much as possible of the case in public, and will hear sensitive matters, such as those relating to the registrant's health, in private.

3.32 Once a decision has been taken to refer an allegation to the FTPC, we will serve the documentation on the registrant and their representative[8].

3.33 We are under a continuing duty to disclose throughout the FTP process. When any new information is received, we consider whether this should be disclosed to the registrant. The presumption will be in favour of disclosure, unless there are public interest reasons against disclosure.

3.34 We will publish the following information on our website prior to the hearing:

3.34.1 the registrant's name;

3.34.2 the registrant's registration number;

3.34.3 the date of the hearing and where it is due to take place;

[8] Rule 29(1), (6) – (8) of the General Optical Council (Fitness to Practise) Rules of Order of Council 2013

3.34.4 the names of the Committee, legal adviser and, when applicable, the clinical adviser; and

3.34.5 details of the allegation will be redacted in some instances (for example, where they relate to health matters).

Outcomes of the FTPC

3.35 We will notify the registrant, the complainant and the Professional Standards Authority (PSA) of the FTPC outcome, along with any relevant organisations or agencies. The outcome will be shared with GOC employees with a defined business requirement.

3.36 As a designated Competent Authority[9], we must inform the appropriate competent authorities of other relevant European states about a professional whose professional activities have been restricted, or prohibited, even on a temporary basis, by the national authorities or the court in the United Kingdom.

3.37 Our website[10] displays the determinations (which include the allegation and the outcome) of our FTP hearings. These are removed after twelve months unless the sanction is still in force.

3.38 The outcome will be attached to the registrant's entry on the GOC Register where the FTPC has given a warning or imposed conditional registration or suspension.

3.39 Where the outcome of a substantive FTP investigation is erasure, suspension, fine or is of significant public interest, we may issue a press release unless there is a public interest reason not to. The press release will not contain information such as health or other matters outside of the public interest. The press release will remain on our website for as long as the determination is displayed.

3.40 Where the outcome of the FTPC shows no findings (where no impairment is found, no facts are proven, and no warning is issued), we will publish this for a period of three months.

3.41 The transcript of a hearing may be requested through the Compliance Team via foi@optical.org. Subject to payment of reasonable costs, we will provide the transcript (redacted as appropriate) of a determination that is on our website.

Registration Appeal Committee

3.42 For registration appeal committee hearings, the same publication and disclosure principles apply.

3.43 We recognise that the public interest may be different in certain cases, for example it may not be in the public interest to publish the spent convictions of individuals who are appealing against refusal of entry to the student register.

---

[9] The European Union (Recognition of Professional Qualifications) Regulations 2015

[10] https://www.optical.org/en/Investigating_complaints/Hearings/past_hearings/index.cfm

3.44 Registration Appeal Committee determinations will be published for 12 months where the appeal is not successful and three months where it is successful, redacted as appropriate.

4. GOC Register

4.1 We publish a searchable online list of all registered optometrists, dispensing opticians, businesses and students. This is a fundamental pillar of a regulated profession. It is an important tool for members of the public and employers to identify registrants that are appropriately qualified and fit to practise.

4.2 The register will reflect any current FTP sanctions or FTPC warnings against registrants. It will also provide a link to further information about the sanctions. Information relating to whether the registrant is on any barred list will not be disclosed.

4.3 The sanction(s) that a registrant has received will be published on the website and will appear on the online register for the duration of the sanction or for twelve months after a fine or erasure.

5. Letter of Good Standing / Certificate of Professional Status

5.1. We are able to provide Letter of Good Standing (LGS) / Certification of Current Professional Status (CCPS) to current and previous registrants upon request. An administration fee of £15 is payable to the GOC for CCPS.

5.2. With consent of the registrant, the LGS/CCPS will include: name; details of current registration status; and registration history.

6. Redaction

6.1 We are committed to balancing individual data rights with publication of information in the public interest and understand that over-redacting can impact on our ability to protect the public.

6.2 Some information may need to be redacted from published documents, including determinations on our website. For example, the names of all witnesses (other than expert witnesses) will normally be redacted unless the public interest requires publication.

6.3 We will redact sensitive or special category information from medical records unless it is relevant to matters that are the subject of our proceedings.

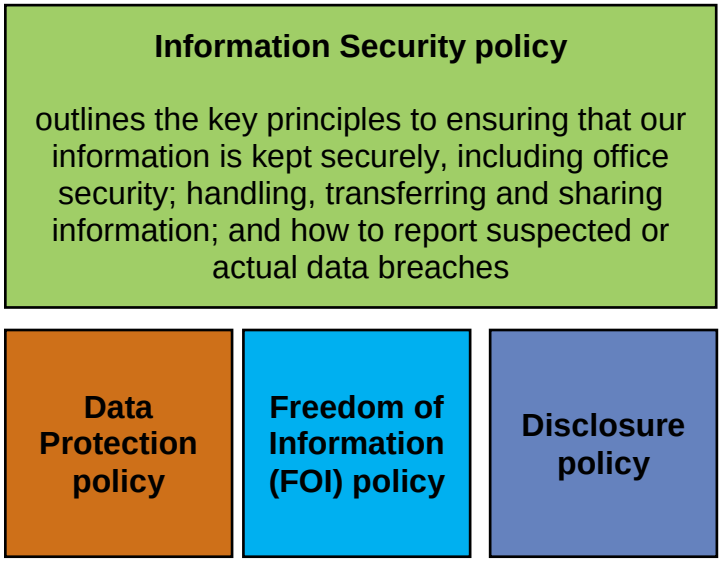
6.4 For more information about how we undertake redaction, please contact the Compliance Team.

7. Internet search engines

7.1 Publications are removed from our website in accordance with this policy, however many interest search engines, such as Google, manage information by ‘caching’. This involves storing a snapshot of a webpage in a database and then refreshing the snapshot periodically. This means that historical GOC webpages

may remain available on internet search engines after they have been removed from our website. In these cases, the individual must contact the internet search engine directly as we have no control over their caches.

Information Security policy



Contents

1. Office security – Office access keys

1.1 All employees, members and those working on our behalf are responsible for ensuring that our premises is left secure and there is no unauthorised access. This includes ensuring that doors are closed, that unknown individuals are challenged and that visitors are accompanied.

1.2 The Facilities department is responsible for ensuring that all access keys are logged when issued to employees and/or members and that they are configured for each person, based on their access requirements.

1.3 Neither employees nor members should automatically be given full access to the office, especially to sensitive areas such as the server room.

2. Office security - Identification (ID) badges

2.1 Employees, members and visitors are required to visibly wear an identification badge and lanyard at all times whilst on our premises.

2.2 All employees, members and visitors must be made aware of the requirement to display their badge at all times by Facilities or HR.

2.3 Employees, members and visitors will be provided with lanyards. Blue lanyards for employees, green lanyards for members and red lanyards for visitors. Only lanyards that are issued by us must be used.

2.4 Employees and members should challenge individuals without visible ID badges. All employees are encouraged to follow this good practice or, at a minimum, report those without ID badges to a manager.

2.5 Members are expected to wear their ID badges when conducting their GOC role at external venues and the GOC offices, for example, when visiting educational providers and within hearings.

2.6 Facilities/Governance maintain a register of ID badges detailing date of issue, losses and destruction for all employees and members, respectively. Facilities/Governance must arrange ID badges in advance of new starters joining the GOC, which are issued as part of the induction process within the first five days of joining.

2.7 New starters working in the office must be issued with a visitor pass daily by Facilities until their ID badge is issued.

2.8 If an employee/member changes their job role, Facilities/Governance must ensure that a new ID badge is issued on the first day of the new role and that the old one is returned, logged and disposed of securely.

2.9 Employees must return their ID badge to HR on their last day of service. Members must return their ID badge within their last week. Facilities/Governance will securely dispose of the ID badge and record its disposal.

3. Reporting loss or theft of ID badge or access key

3.1 Employees must immediately inform Facilities and the Compliance team if their ID badge or Access Key is lost or stolen.

3.2 Facilities will immediately disable an individual's access key and this will be reported as an information security incident (see section 8). The GOC reserves the right to charge individuals £20 for lost access keys.

3.3 Facilities will record of the loss of ID badge and issue another badge.

3.4 As the individual will need to report the loss in order to get a new badge/key, a security incident reporting form only needs to be completed if an actual data breach has occurred (e.g. unauthorised entry to the property) or if the individual has failed to report their badge/key was missing.

4. Visitors

4.1 Reception should be notified by email of visitors at least 24 hours in advance.

4.2 Visitors must report to reception on arrival and complete an entry in the visitor book, which will be stored out of sight.

4.3 Visitors will be provided with a visitor badge and a red lanyard, which they are required to wear in a visible position at all times whilst on GOC premises.

4.4 Visitors who are not working on behalf of the GOC (who have not signed a non-disclosure or confidentiality agreements) must be collected from reception by the receiving employee and accompanied at all times when they are in our offices. They must never be left unsupervised, except for the reception area and public access areas.

4.5 Where it is impossible to accompany visitors at all times, all employees must be made aware of where they are working and the purpose of their visit.

4.6 Visitors must return their visitor badge and lanyard, and complete exit details in the visitor book upon leaving our premises.

5. Handling information

5.1 This section explains our approach to handling information safely. It includes our approach to:

5.1.1 Information Storage (including Clear Desk and Clear Screen);

5.1.2 Printing;
5.1.3 Disposal; and
5.1.4 Templates.

5.2 For further detail regarding these processes please consult the operational guidance, local instructions, or linked policies.

5.3 Information should be treated by all employees, members and those working on our behalf as they would wish their own information to be treated.

5.4 All confidential, personal or special category information in hardcopy or electronic form must be handled securely to mitigate the risk of unauthorised access.

Information Storage – Clear desk, clear screen, locked workstation

5.5 During the day, if the desk is not attended, documents containing confidential, personal or special category information must be put away in cupboards or pedestals.

5.6 Cupboards or pedestals containing confidential, personal or special category information must be closed and locked when not in use or attended. Keys used to access secure cupboards must be returned to key storage and not left unattended.

5.7 Any removable media (e.g. USB sticks, DVDs) and documents containing confidential, personal or special category information must be removed from desks at the end of each working day and kept securely.

5.8 Computers must be ‘locked’ when the desk is unoccupied, and shut down at the end of the working day.

5.9 Care must be taken that the information displayed on all electronic devices is kept confidential, especially in public areas or public transport.

Printing

5.10 When printing confidential, personal or special category information the ‘locked’ printing option must be used and the individual printing must be in attendance.

5.11 Printers must be cleared of papers as soon as they are printed to make certain that confidential, personal or special category documents are not left in printer trays.

Disposal

5.12 Confidential, personal or special category documents, when no longer required, must be safely disposed of in confidential waste bins and care taken to ensure that the documents are fully inserted and not retrievable from the bins.

5.13 Meeting rooms must be immediately cleared of any documents containing confidential, personal or special category data at the end of each meeting, this includes wiping down whiteboards and disposing of flip charts.

5.14 For more information about disposal of archived information, please consult our Data Protection policy.

Templates

5.15 Any templates used must be blank. Previously amended versions of templates must not be used as the base template, due to the risk of personal information being incorrectly included in the next use.

6. Transferring and sharing information safely

6.1 This section is about how to transfer data securely. For further information about when to share and when not to share information please refer to our Data Protection policy and Disclosure policy.

6.2 Always ensure the level of security is appropriate to the nature of the data being transmitted.

Transporting / on the move

6.3 Care must be taken at all times to ensure that all electronic and physical information is transported securely. This includes transporting laptops which are shut down so that the encryption code is still required, and taking the appropriate measures such as putting sensitive documents in a lockable file for transport.

Posting

6.4 All post must be checked by the sender, prior to sending. The check must include:

- 6.3.1 verification of the address on the envelope, letter and the address held on file;
- 6.3.2 verification that the information included is the correct information for the addressee;
- 6.3.3 that any redaction has been fully completed and verified by another person; and
- 6.3.4 that no further information has been included, due, for example, by an error in printing, scanning or template use.

6.4 When posting confidential, personal or special category information, use non-rip envelopes or double envelopes (ensuring name and address is on both envelopes), mark ‘private and confidential’ or ‘for addressee only’, and send via recorded delivery or courier.

6.5 In order to facilitate the appropriate management of business, in general Facilities may open any post that we receive at the GOC in order to establish the intended and appropriate receiver as long as it is reasonably addressed to the GOC.

6.6 For post marked ‘private and confidential’ or ‘for recipient only’, which is addressed to the GOC, it would be handed to Facilities Manager to open, sign and record a reference. In their absence, our Facilities team would seek authorisation from Head of Finance or Director of Resources.

Emails

6.7 All emails must be checked by the sender, prior to sending. The check must include:
- 6.7.1 verification of the email address (sending a test email first if necessary)
- 6.7.2 verification that the information included is the correct information for the addressee;
- 6.7.3 that any redaction has been fully completed and verified by another person; and
- 6.7.4 that no further information has been included, due, for example, by an error in printing, template use, or previous email chain.

6.8 When sending emails, it is important to consider:
- 6.8.1 who are the recipient(s), are they internal/external;
- 6.8.2 might the message be intercepted if external;
- 6.8.3 are previous emails included in the correspondence still relevant;
- 6.8.4 do attachments require password protection or encryption; and/or
- 6.8.5 the security marking of the email.

6.9 For additional security, senders should consider switching off their auto-fill on email addresses in Outlook. This can be made mandatory by Information Asset Owners.

6.10 Senders should also consider including protective markings in the subject and body of the email and as the email setting, as appropriate.

6.11 For further information on electronic security measures, please refer to the IT policy.

Verbal/over the phone

6.12 Users should ensure that they are not being overlooked or overheard if working on or discussing GOC business in public.

6.13 Telephone calls can often lead to unauthorised use or disclosure of personal data. It is mandatory to complete the following checks before releasing the data:
- 6.13.1 Verifying the caller’s identity – by asking questions only they would know, or by emailing or calling them back on the email/number we have on our IT system.
- 6.13.2 If they are not the data subject and are requesting detail about someone else, you must not disclose information pertaining to the data subject, unless you have explicit consent from the data subject. If in doubt, ask them to put their

request in writing, or take their name and number and seek further advice with the Compliance Team or your line manager.

7. Removable media

7.1 We recognise that there are a number of risks associated with handling information, in particular those associated with the use of removable media, in order to conduct our functions. For this reason, removable media devices are prohibited unless there is a valid request that demonstrates a valid business use, which outweighs the associated risks and vulnerabilities, and the request has been approved in line with the IT policy and process.

7.2 Removable media includes, but is not limited to: media Cards; CDs; DVDs; external hard drives; USB memory sticks (also known as pen or flash drives); any other electronic storage devices.

7.3 Removable media must be treated like it is confidential, personal or special category information and in line with the Data Protection Policy.

7.4 The process for obtaining and using removable media is managed by our IT department. Individuals must consider alternative, more secure arrangements, prior to requesting to use removable media.

7.5 Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss, including encryption.

7.6 Only removable media devices supplied by our IT team may be used. Personal (non-GOC) removable media devices must not be used to store any GOC information and must not be used with any GOC-owned equipment.

7.7 Removable media provided by the GOC must not be used for anything other than the approved purpose. Only data that is authorised and necessary to be transferred should be saved on a removable media device.

7.8 Removable media devices must not be used for archiving or storing records as an alternative to the GOC network.

Encryption

7.9 All data stored on removable media must be encrypted according to the GOC encryption standards, as provided by IT.

7.10 All data that is transferred to a third party via removable media must be on a GOC-supplied encrypted device.

7.11 Virus and malware checking software approved by IT must be operational on both the machine from which the data is taken and the device onto which the data is to be loaded.

8. Reporting an information security incident or near-miss

8.1 All employees, members and those working on our behalf are expected to immediately report actual, suspected or potential breaches of information security. On discovery of the incident to the person who has discovered the incident must report it to their line manager (or their respective line managers if they are not available) and the Compliance team immediately and via foi@optical.org.

8.2 Dependant on the nature of the incident, the reporter may also need to inform the following person or people so that the matter can be most swiftly and appropriately managed:

Type of incident	Report to	Examples
IT / Cyber	Director of Resources and IT	Virus, phishing attempt, lost laptops, iPads or mobile phones, compromised password
Physical security	Facilities Manager	Breaches of physical security – unauthorised entry on site, lost access key.

8.3 This may include invoking the Business Continuity Plan or other policies.

8.4 Within 24 hours of becoming aware of the incident, the reporter must submit a security incident report form[11] to the Compliance team. Failure to report within this timescale may be considered a disciplinary offence.

8.5 This is important because if the incident is 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.

8.6 The Compliance team or the department manager will complete an investigation into the incident. If the incident is serious, conducting a full investigation in accordance with our internal Investigation policy may be considered.

8.7 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 Compliance team.

8.8 The Compliance team will ensure that the following stages of breach management are completed in a timely manner, considering the ICO guidance on breach management[12]:

[11] H:\01 Shared Resources\01.03 Documents\01.03.02 Forms
[12] https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

8.6.1 containment and recovery;
8.6.2 assessment of ongoing risk;
8.6.3 notification of breach; and
8.6.4 evaluation and response.

8.7 All Security Incident Reports will be signed off by the Data Protection Officer (DPO) or deputy once an investigation has been completed.

8.8 The DPO will decide whether any breach needs to be reported to the ICO, considering the ICO's guidance[13] and will oversee its reporting, where required. Any ICO-reportable breaches need to be reported to the ICO **within 72 hours** of us becoming aware. Failure to do so can result in an automatic fine from the ICO.

8.9 Remedial and permanent measures to mitigate risk of reoccurrence will be implemented by the appropriate department(s) who will be supported by the Compliance Team.

8.10 The Compliance Team will record all actions taken and lessons learnt from the incident or near miss and will ensure these are periodically distributed within the organisation for continued learning and awareness.

[13] https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf