Data Sharing Agreement Policy

Our data Sharing Agreement policy outlines our approach to complying with the Data Protection Act and UK GDPR and other regulations when it comes to sharing 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 have a legal responsibility to ensure that our use of personal data is lawful, and properly controlled and that an individual's rights are respected. This includes ensuring that our partner organisations also abide by the legislation.

1.2 This policy forms part of our Information Governance Framework and sets out a process and agreement in order to facilitate sharing of all relevant personal sensitive, and non-personal data between public, private, and voluntary sectors to ensure organisations are able to complete their functions effectively.

1.3 To carry out our statutory functions and support other public bodies to carry out theirs, we rely on efficient information sharing with other parties. Failure to adhere to this policy and creating unnecessary barriers to sharing information will detriment our ability to complete our statutory functions.

1.4 Each partner to this policy and agreement should ensure that all their employees who are affected by it are:

- aware of and understand the data sharing agreements' contents; and
- agree to work within the rules set out in the agreement and protocol.

1.5 Each partner should ensure that revisions to the Data Sharing Agreement are signed in good time, which must be before any information sharing takes place.

1.6 By entering in a Data Sharing Agreement with the GOC, both parties are committing to achieve appropriate compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

1.7 Both parties are expected to promote and develop employee awareness of the key requirements of information sharing. This must be supported by the production of appropriate policies and guidance where required that will be made available to all employees via each organisation's internal communication methods.

2. Purpose

2.1 The purpose of this policy is to provide a framework for lawful information sharing to ensure we and our partner organisations can complete their duties effectively. The policy will establish and regulate working practices between ourselves and our partner organisations and provide guidance to ensure the secure transfer of information and that information shared is for justifiable legal purposes.

2.2 The policy aims to;

- set out the security and confidentiality laws and the principles of information sharing;
- increase awareness and understanding of the key issues regarding information sharing;
- agree how to share information lawfully;

- support a process that will monitor and review all information flows;
- encourage safe and efficient sharing of information; and
- protect our organisation from accusations of wrongful or illegal use of personal data.

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. Glossary of Terms

UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018)	The legislation which sets out a data subject's individual data protection and data privacy rights.
Anonymised data	Data which, even when combined with other information from different agencies, does not identify an individual, either directly or by summation.
Confidentiality	Data, which is provided in confidence, without the implicit permission of publication.
Data Sharing Agreement	The specific agreement which sets out the purposes of sharing the information.
Data subject	The person who is the subject of the personal information.
Destruction	The permanent destruction of information.
Freedom of Information (FOI)	The legislation within the Freedom of Information Act 2000 (FOIA) gives people the right to request information from public authorities.
Information Commissioner's Office (ICO)	The organisation that oversees compliance with the UK GDPR, DPA 2018 and FOIA.
Information	There are three Information/data categories referred to within this policy: Corporate, Personal Data, and Special Category Data.
Confidential information	Confidential information means any non- public information pertaining to the GOC.

Personal Data	The term 'personal data' refers to any data held either manually or as electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that data. Personal data is data relating to a living individual who can be identified from those data, and any other information which is in the possession of or is likely to come into the possession of the data controller (person or organisation collecting that information).
IT	Information Technology.
Partner, partnership organisation	Any organisation which enters into an agreement or works with the GOC.
Public interest	Within Information Governance, this is generally considered as something which serves the interest of the public.

5. Terms for Sharing Information

5.1 Each partner organisation is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this policy, including personal and non- personal information.

5.2 Partner organisations must have the appropriate Information Governance policies and processes in place.

5.3 The data sharing agreement should contain hyperlinks or annexes of partner Information Security policies.

5.4 The Security requirements will not be included in the individual data sharing agreement except where they are unique to that Agreement. This will ensure requirements are kept current, as notified, and avoid errors arising from having more than one copy of a partner's standard requirements.

5.5 It is accepted that not all partners will have security classifications in place, however partners should ensure that the minimum standards of security that they require are agreed with partners with whom their information will be shared; this must be specified in the data sharing agreement.

5.6 The partner organisation originally supplying the information should be notified of any breach of confidentiality or incident involving risk or breach of the security of information.

Third Parties

5.7 Partner organisations should ensure that their contracts with external service providers include a condition that they abide by their rules and policies about the protection and use of confidential information.

5.8 Re-use of information is not authorised unless specifically agreed upon within the data sharing agreement.

Anonymised Data

5.9 Organisations must ensure that anonymised data, especially combined with other information from different agencies, does not identify an individual, either directly or by summation.

5.10 Anonymised data about an individual can be shared without consent (subject to certain restrictions regarding health/social care records), in a form where the identity of the individual cannot be recognised.

Pseudonymised Data

5.11 The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

5.12 Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. Whilst you can tie that reference number back to the individual if you have access to the relevant information, you put technical and organisational measures in place to ensure that this additional information is held separately.

5.13 Pseudonymising personal data can reduce the risks to the data subjects and help you meet your data protection obligations.

5.14 However, pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data and remains personal data and within the scope of the UK GDPR.

Non-Personal Data

5.15 Partner organisations should not assume that non-personal information is not sensitive and can be freely shared. This may not be the case and the partner from whom the information originated should be contacted before any further sharing takes place.

Sharing Personal Data

5.16 Employees should only be given access to personal data where there is a legal right for them to perform duties in connection with the services they are employed to deliver.

5.17 Personal data shall not be transferred to a country or territory outside the UK without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data, including consent.

5.18 Personal data should only be shared where a specific lawful basis has been established i.e., to perform our task in the public interest, a legal obligation, or where consent has been obtained.

5.19 Consent has to be freely given and unambiguous signified by written communication between the organisation and the data subject. If the data subject does not respond this cannot be assumed as implied consent. When using a special category of personal data, explicit consent must be obtained subject to any existing exemptions. In such cases, the data subject's consent must be clear and cover items such as the specific details of processing, the data to be processed, and the purpose for processing. The consent must also be up to date in order to be relied upon.

5.20 Specific procedures will apply where the data subject is either not considered able to provide informed consent because of either the age or where the data subject has a condition that means the data subject does not have the capacity to give informed consent. In these circumstances, the relevant policy of the partner organisation should be referred to.

5.21 If consent is used as a form of justification for disclosure, the data subject must have the right to withdraw consent at any time.

Withdrawing Consent

5.22 Partner organisations must be aware that a data subject may withdraw consent for the processing of their personal information. In this case, processing can only continue where a reasonable justification or condition applies (see paragraph 5.8.1).

5.23 Where the partner organisations rely on consent as the condition for processing personal data then withdrawal means that the condition for processing will no longer apply. Withdrawal of consent should be communicated to Partner Organisations and processing ceases as soon as possible, where applicable.

Sharing Without Consent

5.24 Consent is not the only means by which personal data can be disclosed. Under the UK GPDR and the DPA 2018 in order to disclose personal data at least one condition in schedule two must be met. To disclose sensitive personal data at least one condition in both schedules, two and three must be met.

5.25 Schedule two of the UK GDPR and DPA 2018, conditions relevant for the first principle: Processing of any personal data, states personal data may be processed if:

- The data subject has given consent to processing the data.
- The processing is necessary for the administration of justice.
- The processing is necessary for the exercise of any function of the crown, a minister of the crown, a government department; or
- The processing is necessary for any other functions of a public nature exercised in the public interest by any person.

5.26 Where a partner organisation has a statutory obligation to disclose personal data then the consent of the data subject is not required, but the data subject should be informed that such an obligation exists.

5.27 If a partner organisation decides not to disclose some or all of the personal data, the requesting authority must be informed. For example, the partner organisation may be relying on a lawful exemption from disclosure or on the inability to obtain consent from the data subject.

Restrictions on the use of shared information

5.28 All information, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure, as defined in the relevant data sharing agreement unless obliged under statute or regulation, or under the instructions of a court or as agreed elsewhere. Therefore, any further uses made of this data will not be lawful or covered by the data sharing agreement.

5.29 Restrictions may also apply to any further use of non-personal information, such as commercial sensitivity or prejudice to others caused by the information's release, and this must be considered when considering the secondary use of non-personal information. If in doubt, the information's original owner must be consulted before any secondary use.

5.30 Additional statutory restrictions apply to the disclosure of certain information e.g., criminal records and health records. Specific information about these must be included in the relevant Data Sharing Agreement.

6. Responsibilities

6.1 Each partner organisation is responsible to ensure that all employees accessing information shared under this policy and data sharing agreement are trained to a sufficient level that enables them to undertake their duties confidently, efficiently, and lawfully. Refresher training must be completed at a minimum every two years.

6.2 Each partner organisation must ensure that any of its employees accessing information under a data sharing agreement follow the procedures and standards that have been agreed upon and incorporated within this Data Sharing Agreement policy and any associated Data Sharing Agreements.

6.3 Each partner must ensure that there is compliance with the data sharing agreement and policy. Should the partner wish to make amendments to the data sharing agreement or update the annexed material, they must do so in conjunction with the other partner(s) and must not make any changes without informing the other partner.

Individual Responsibilities

6.4 Every individual handling the information shared from this policy:

6.5 is personally responsible for the safekeeping of any information they obtain, handle, use and disclose, and must understand how to process information lawfully.

6.6 should uphold the general principles of confidentiality, following the guidelines set out in this agreement, seeking advice when necessary.

6.7 Has an obligation to request proof of identity or take the necessary steps to validate the authorisation of another, before disclosing any information requested under this agreement and associated data-sharing agreements.

7. Information Quality

7.1 Information quality needs to be of a standard fit for the purpose information is to be used for, including being complete, accurate and up to date as required for the purposes for which it is being shared. Without this any decision made on the information may be flawed and inappropriate actions may result.

7.2 Partner organisations are expected to ensure personal data and sensitive personal data that it holds is processed in accordance with DPA principles: this includes ensuring that data is accurate, complete, and up to date and is not kept for any longer than is necessary.

7.3 All partner organisations are expected to provide undertakings that information meets a reasonable quality level for the proposed purposes for which it is being shared and be able to evidence this.

8. Compliance

8.1 Partner organisations accept responsibility for independently or jointly auditing compliance with data sharing Agreements in which they are involved within reasonable timescales. Each partner is able to ask the other to demonstrate compliance with data legislative requirements, and data sharing may cease during this time.

8.2 Should any partner fail to adhere to the data legislation, or the agreement set out within this policy, the data sharing agreement may cease at any time.

8.3 If a data breach occurs during or after sharing the information with a partner organisation, the organisation should report it to the partner organisation contact immediately. The organisations are expected to work together to manage any data breaches.

8.4 Failure to respect confidentiality and privacy is unlawful and could lead to dismissal. Criminal proceedings might also be brought against that individual.

8.5 Each partner organisation will keep each of the other partners fully indemnified against any and all costs, expenses, and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents, or any other person within the control of the offending partner of any personal data obtained in connection with this agreement.

9. Transparency

9.1 We reserve the right to publish details of our sharing agreements on our website. To do so, we may remove any personal data which is listed in the agreement.

9.2 All previous Data Sharing Agreements will be stored on our system and will be kept secure and retained as per our retention policy.

9.3 Should you wish to reuse any of our public information in this manner, please email the Information Governance Officer at IG@optical.org.

10. Process for Implementing a Data-Sharing Agreement

10.1 When a Data Sharing Agreement needs to be implemented it is important that this has been approved by all appropriate staff.

10.2 Information Governance should be informed in the early stages of creating the agreement to ensure that we have a legal basis to share the information and that the appropriate steps are being taken to securely share the information.

10.3 The data sets should then be reviewed to ensure that we are only processing what is necessary for the task.

10.4 This should then be agreed by the Asset Owner who has overall responsibility of the data and the SIRO.

10.5 This should then be sent to the organisation that wishes for us to use a Data Sharing Agreement for them to agree and sign the document.

10.6 Once the Sharing Agreement has been signed by the third-party organisation the Asset and the SIRO must sign the document and a copy kept for our records.

Annex 1 – Data Sharing Agreement Template

Name of agreement:	
Purpose of agreement:	

Name of Organisation - Partner 1	**General Optical Council**
Partner 1 - Agreement owner name and contact details	
Name of Organisation - Partner 2	
Partner 2 – Agreement owner name and contact details	
Date and signature of agreement: Partner 1	
Date and signature of agreement: Partner 2	
Location of this agreement	**Website address:**
Agreement start date:	
Agreement end date:	*(Applicable for projects)*
Date of next review:	
Agreement status	*Draft, live, expired*
Amendments:	

1. Purpose of the Data Sharing Agreement

1.1. This agreement has been developed to ensure information sharing between the aforementioned parties has an effective governance structure.

1.2 This agreement does not give complete freedom for the wholesale sharing of information. Information sharing must take place within the constraints of the law, relevant guidance, and service-specific requirements.

1.3. Sharing is underpinned by the ethos of informed consent and client confidentiality being tantamount to any information sharing between agencies.

1.4. This agreement will be underpinned by the operational agreements as designed to meet the specific needs of the project study and to assure any information sharing is undertaken within the realms of current legislation and legal frameworks.

2. Principles

2.1 This agreement outlines the principles and operational guidelines for how information and data is securely managed between the organisational partners.

2.2 The following key principles guide the sharing of information between the partners:

- Partner organisations endorse, support, and promote the accurate, timely, secure, and confidential sharing of both person identifiable and anonymised information for the sole purpose of this agreement.
- Partner organisations are fully committed to ensuring that if they share information, it is in accordance with their legal, statutory, and common law duties, and, that it meets the requirement of all additional guidance.
- Partner organisations have in place policies and procedures to meet the national requirements for Data Protection, information security, and confidentiality. The existence of, and adherence to, such policies provide organisations with confidence that information shared will be transferred, received, used, held, and disposed of appropriately.
- Partner organisations acknowledge their 'Duty of Confidentiality' to data subjects. In requesting the release and disclosure of information from other organisations, employees will not seek to override the procedures which each organisation has in place to ensure that information is not disclosed illegally or inappropriately. This responsibility also extends to third-party disclosures and any proposed subsequent re-use of the information that is sourced from another organisation must be approved at the source.
- Only data which is needed and relevant to the purpose will be shared.
- This will be on a 'need to know basis.
- Partner organisations will ensure that all relevant employees are aware of and comply with, their responsibilities regarding both the confidentiality of information about people who are in contact with their organisation and the commitment of the organisation to share information.
- All relevant employees must be aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action.
- Partner organisations are responsible for putting into place effective procedures to address complaints relating to the disclosure of information, and information about these procedures should be made available to service users.
- Partner organisations must declare where they will process the information, and ensure the information is within the UK.

3. Consent

3.1 To facilitate the effective success of the data sharing, explicit consent of the data subjects is mandatory. As a minimum, data subjects will be informed that information will be shared across partner organisations.

3.2 Explicit consent to share the information will be sought, verbally or written, unless it may detriment the completion of a statutory function.

3.3 Partner organisations are required to have clear policies on the purpose of processing information and the storage and retention of information, including the maximum retention period and a secure process of destruction.

4. Process

4.1 In addition to the expectations set out in the Data Sharing Agreement Policy and elsewhere within the data sharing agreement, the specific processes, expectations, and/or requirements (for sharing information for the purposes outlined above) are:

Partner 1:
• • • •

Partner 2:
• • • • •

4.2 Please ensure that details regarding the following are included within the above:

- how consent will be obtained (if applicable).
- how the data will be used.
- when the data will be destroyed.
- where the data will be processed and stored (i.e. within the UK or abroad);
- if the data will be presented or published, how will this be done, and to whom; and
- if any other third parties are involved, please provide other relevant data-sharing agreements or equivalent.

5. Supporting Policies, Procedures, and Guidance

5.1 All partner organisations are required to share information lawfully, securely and within the relevant guidance. Partners must ensure they have appropriate policies regarding:

- Data Protection.
- Records retention and disposal.
- Confidentiality.
- Information security and Incident management; and
- Caldicott principles (if required).

5.2 These policies must cover manual, verbal, and electronic information.

6. Information Breaches or Near-miss incidents

6.1 Any incidents where the shared personal, sensitive, or confidential data is compromised, lost, disclosed or the confidentiality is breached or potentially breached must be immediately reported to your manager, you will then be asked to complete an incident form. This must then be sent to IG@optical.org, who will then advise on the next steps. Where applicable providing partners should be notified of the data breach and steps taken to ensure this does not happen again.

6.2 The point of contact to report breaches is: IG@optical.org

7. Audit and Review

7.1 All organisations accessing data must have appropriate governance and risk assessment measures in place, to assure the safe storage, access, and utilisation of identifiable data.

7.2 Policies should be available for audit purposes with evidence of clear review dates.

7.3 Where not already established, processes will be set up in each organisation to adopt a risk management approach to breaches in relation to the implementation of this agreement.

7.4 It is the responsibility of both partners to review the data-sharing agreement before its expiry or next review date. Should the data-sharing agreement expire, data must not be shared until a new agreement is in place.

Annex 2 – Non-Disclosure Agreement Template

Non-Disclosure Agreement

Date: Parties:
[COMPANY NAME], a company registered in England under the company number [COMPANY NUMBER] whose registered address is [REGISTERED ADDRESS] (hereinafter the "Recipient")
And
The General Optical Council, a charity registered in England and Wales under the charity number 1150137 whose registered address is at 10 Old Bailey, London, EC4M 7NG (hereinafter the "Discloser")

1. The Discloser intends to disclose confidential information to the Recipient for the purpose of [PUT OVERALL PURPOSE].

2. All information sent by the Discloser to the Recipient or collected by the Recipient in their capacity as defined in clause 1 is not to be disclosed without first obtaining the written agreement of the Discloser and shall be treated as confidential. Such information shall hereinafter be "Confidential Information".

3. Any information, material, or data received by the Recipient, including from third parties or subcontractors, relevant to instructions between the Discloser and Recipient, should not be disclosed without the prior written agreement of the Discloser.

4. The Recipient undertakes not to use the confidential information for any purpose except for the purpose defined in clause 1, without first obtaining the written agreement of the Discloser.

5. The Recipient undertakes to keep the Confidential Information secure in compliance with UK General Data Protection Regulation and Data Protection Act 2018 including data defined as Special Category Data and provide assurance of the policies and procedures in place.

6. The Recipient undertakes to report any potential or actual breach of information security immediately to the Discloser, via IG@optical.org, and to provide further details regarding any incident and take appropriate action as requested by the Discloser.

7. The undertakings in clauses 2, 3 and 4 above apply to all information disclosed by the Discloser to the Recipient, regardless of the way or form in which it is disclosed or recorded.

8. Nothing in this Agreement will prevent the Recipient from making any disclosure of the Confidential Information required by law or by any competent authority. The Recipient must inform the Discloser if any material is to be so disclosed.

9. The Recipient will, on request from the Discloser, return all copies and records of the Confidential Information (hardcopy, digital, or otherwise) to the Discloser within one month of the request and undertakes not to retain any copies or records of the Confidential Information as instructed.

10. The undertakings in clauses 2, 3, and 4 will remain in force upon determination of any contract or agreement between the Recipient and Discloser.

11. This Agreement is governed by and is to be construed in accordance with, English law. The English Courts will have non-executive jurisdiction to deal with any dispute which has arisen or may arise out of, or in connection with, this Agreement.

Name Signature Date
Signature of witness

Date.....

Name of witness.....

Address of witness.....