**Information Rights Complaints Policy**

|  |  |
| --- | --- |
| Responsible Officer | Interim Director of Finance |
| Author | Head of IG&RM / Data Protection Officer |
| Date effective from | September 2023 |
| Date last amended | September 2023  |
| Review date | September 2026 |

# Introduction

1. Data protection legislation (the Data Protection Act 2018 and the UK General Data Protection Regulation (UKGDPR)) is the framework in which organisations operate when processing personal data relating to identifiable and living individuals. This legislative framework, also known as the data protection regime, governs organisations’ use of personal data and provides a mechanism for individuals to exercise their individual rights in relation to how organisations use their data.
2. Individuals’ rights regarding the processing of their personal data are set out in Articles 15 to 22 of the UKGDPR. These are:
* The right of access (Article 15)
* The right to rectification (Article 16)
* The right to erasure (Article 17)
* The right to restrict processing (Article 18)
* The right to be notified regarding rectification or erasure of personal data or restriction of processing (Article 19)
* The right to data portability (Article 20)
* The right to object (Article 21)
* The right to object to automated decision-making including profiling (Article 22)
1. These rights are not universal and certain conditions must be met in order for the rights to be engaged. For example, an organisation is not required to delete all data relating to an individual where the lawful basis for processing the individual’s personal data is the organisation’s public task.
2. Organisations processing personal data are required to adhere to the data protection principles set out in Article 5 of the UKGDPR. The seven data protection principles underpin how personal data should be processed within the organisation, and embody lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability.
3. NICE is required by the UKGDPR to appoint a Data Protection Officer who independently oversees the organisation’s compliance with data protection legislation by monitoring internal data processing activities. In addition, the Data Protection Officer is required to uphold individuals’ rights and ensures that the organisation fulfils its duties by operating within the confines of the law. NICE’s Data Protection Officer is the Head of Information Governance and Records Management.

# Scope

1. This policy sets out NICE’s process for investigating complaints made about the organisation’s compliance with data protection legislation and concerns raised about the organisation’s possible infringement of individual rights specified in the UKGDPR.
2. It applies to all personal data held by NICE ranging from patient identifiable data to personal data of staff, suppliers, stakeholders, and any other individuals who work with or contact NICE.
3. This policy sets out how NICE will:
	* Investigate complaints or concerns about how personal data is processed at NICE from internal and external parties, including but not exclusively employees, members of the public and partner organisations.
	* Enable individuals to exercise their individual rights and how complaints relating to the implementation of these rights are handled.
	* Investigate alleged breaches of the Data Protection Act and/or UK GDPR in relation to the processing of personal data.
4. This policy does not extend to complaints about access to non-personal data held by NICE. Access to such information held by NICE is governed more generally by Freedom of Information law and the complaints procedure surrounding this process is covered in the Freedom of Information Policy and Complaints Procedure. Similarly, this policy does not extend to investigations concerning breaches of non-personal data (commercial in confidence or academic in confidence data).

# Responsibilities

1. The Information Governance and Records Management (IG&RM) team is responsible for administering information rights requests and co-ordinates the process. The team liaises directly with the requester surrounding the progress of their request, determines whether a request is valid, co-ordinates the task of locating information held within the organisation, and applies any legal exemptions to the disclosure of information in the case of subject access requests. Where enquiries or complaints regarding the processing of personal data are received, these are forwarded to the Data Protection Officer.
2. The Deputy Data Protection Officer is the senior member of the IG&RM team responsible for the co-ordination and despatch of a response to the data subject where an individual rights query is made. The Deputy DPO oversees the handling of the request and ensures that the procedures outlined in the standard operating procedure are followed. The Deputy Data Protection Officer may seek advice and assistance from the Data Protection Officer for the purposes of handling particularly complex or sensitive information rights requests. The complexity and sensitivity of a request will be determined on a case-by-case basis by the Data Protection Officer and Deputy.
3. The Data Protection Officer maintains strategic oversight of the completion of information rights requests and is kept abreast of progress by the IG&RM team. The Data Protection Officer is responsible for reviewing the initial handling of a request in the event that the data subject is dissatisfied with the response they receive from the IG&RM team and requests a review. Should the data subject remain dissatisfied with the outcome of the DPO’s review, they can escalate this to the Information Commissioner’s Office (ICO).
4. The Data Protection Officer is also the first point of contact for anyone wishing to lodge or discuss any concerns about the organisation’s procedures governing the processing of personal data, either related directly to themselves or another third party. Where the issue at hand concerns a breach of personal data as specified in the UKGDPR, the Data Protection Officer will adhere to the relevant part of the Data Breach Reporting and Management Policy.

#  Handling information requests

**Information rights**

1. Individuals wishing to exercise their information rights should contact the IG&RM team at IGandRMSupport@nice.org.uk. The team will verify the identity of the data subject before initiating the request process. Where a third party makes contact with NICE on behalf of a data subject, the appropriate authorisation to act on the data subject’s behalf will be checked.
2. The IG&RM team will endeavour to respond to an information rights request within the statutory time period; which is one month for subject access requests and as soon as practicable for other requests such as the right to rectification, for example.
3. In the response to the data subject, the IG&RM team will set out what action the data subject should take in the event that they have a further query regarding the outcome of the request or the information they have been supplied with and/or are dissatisfied with the outcome. The initial response to the data subject will explain how NICE’s Data Protection Officer should be contacted about any further queries or complaints. Further queries/escalations to the DPO must be made in writing to the DPO at:
* Email: DPO@nice.org.uk
* Post:

Data Protection Officer

National Institute for Health and Care Excellence

Level 1A

City Tower

Piccadilly Plaza

Manchester

M1 4BT

1. Where a complaint, concern or query about how an information rights request is made, the DPO will review the previous handling ofem the request and consult with all relevant, internal parties, where necessary. The DPO will respond directly to the data subject (or third party acting on their behalf) regarding the outcome of their review. The response will usually be sent within twenty working days of the query or complaint being received. The data subject will be advised at the earliest opportunity if, exceptionally, further time is required for the response.
2. Where the data subject remains dissatisfied with the response provided by the DPO, the DPO will advise the individual to contact the Information Commissioner’s Office for further advice as the final point of escalation. This concludes NICE’s involvement with the enquiry.

**Data processing complaints**

1. Where any party has concerns about NICE’s processing of personal data, the Data Protection Officer should be contacted directly and in the first instance. Depending on the scope of the enquiry and concern lodged, the Data Protection Officer will carry out some preliminary investigations into the matter and consult with the Deputy Data Protection Officer if required.
2. Where the concern/issue has been raised by an internal party at NICE, the DPO will endeavour to respond as soon as possible once the fact-finding stage has been completed. Concerns of this nature will be treated informally. Where the concern/issue has been raised by an external, third party, the DPO will liaise with the third party regularly to keep them informed of progress in completing their enquiries and will respond formally. The response will usually be sent within twenty working days of the query or complaint being received. The third party will be advised at the earliest opportunity if, exceptionally, further time is required for the response.
3. In the event that the enquirer is dissatisfied with the outcome of the DPO’s investigation, the DPO will review the initial handling of the request before advising the enquirer to contact the Information Commissioner’s Office for further advice if they remain dissatisfied.

**Personal Data breach complaints**

1. Where the issue at hand concerns a breach of personal data as specified in the UKGDPR, the Data Protection Officer will investigate and adhere to the relevant part of the Data Breach Reporting and Management Policy. A personal data breach is defined under the UK General Data Protection Regulation (UK GDPR) Article 4 (12) as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes.
2. An example of a breach of the UKGDPR which would be investigated under the Data Breach Reporting and Management Policy, could be an allegation that the personal data of an individual had been unlawfully shared or accessed by an unauthorised third party, the result of which has caused the data subject distress or harm and ultimately had a detrimental effect. This would be a breach of confidentiality, but other such breaches could concern the integrity or availability of an individual’s personal data.
3. The Data Protection Officer is required to liaise with the data subject (or their representative) directly and will conduct their investigation independently, free from the influence of any internal parties at NICE. That said, it may be necessary for the DPO to consult with other internal parties at NICE, such as HR or colleagues within the Digital, Information and Technology (DIT) directorate, in the event that the data breach complaint is connected to other complaints in progress within the organisation, so that the DPO is mindful of the wider context of the issue at hand.
4. As part of their investigation, the Data Protection Officer may conduct interviews with third parties at NICE who may be involved with the breach as part of a fact-finding exercise. The DPO is required to examine the evidence purporting to any alleged breach to determine whether a breach has occurred and recommend remedial action to minimise the effects of any such breach, if this is a viable option at the time the incident is reported. The Data Protection Officer will afford greater weight to the recorded evidence to hand as part of their investigation which will ultimately inform the outcome.
5. Where the Data Protection Officer concludes that a breach has occurred, the details will be recorded in the data breach register and reported to the Information Governance Steering Group (IGSG). Where the threshold of harm and risk to the rights and freedoms of the data subject is met as an effect of the data breach, the Data Protection Officer will determine whether reporting to the ICO is required. The DPO will make this decision subjectively and independently, in consultation with the Deputy DPO, if required. The data subject will be informed of the outcome of their complaint/concern once the DPO has reached their conclusion.
6. Where the data subject is dissatisfied with the outcome of their complaint, the DPO may consider reviewing their initial response. Where the DPO’s review does not change the outcome of the complaint and/or the data subject remains dissatisfied, the data subject will be required to contact the Information Commissioner’s Office for further advice.

# Information Rights requests and complaints made by data subjects with an employee/employer relationship to NICE

1. When an employee makes a complaint, NICE will ensure the process complies with the ACAS code of practice and the NICE Grievance Resolution procedure. Where a complaint relates solely to a possible breach of information rights, an investigation will be conducted under the Information Rights Complaints Policy. Where a complaint is made under stage 2 of the grievance resolution procedure, which is multifaceted and includes a possible breach of information rights, the Commissioning Manager for the grievance will ask the data protection officer to complete an investigation report into the aspects of the grievance which relate to a possible breach of information rights. An investigating Manager will still be required to investigate the other complaints raised. Both reports will then be considered at a subsequent grievance hearing. For stage 2 of the Grievance Resolution Procedure, the data protection officer will take on the role of Investigating Manager when requested to complete an investigation by a commissioning manager, A decision tree and Process map are provided as an appendix to this policy to support clarity as to which procedure will be followed.

# Review

1. This policy will be reviewed every three years.

### Related policies

* Freedom of Information Policy and Complaints Policy
* Data Breach Reporting and Management Policy
* Individual Rights procedure
* Subject Access Rights Standard Operating Procedure
* General complaints policy and procedure
* HR Grievance Policy

**Version control table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Replaces** | **Comment** |
| 1.0 | September 2023 | Head of IG / DPO | New policy | Complements the Freedom of Information and Complaints Policy.  |
| 1.1 | November 2023 | Information Governance Manager / Deputy DPO | Policy amended for clarification purposes  | Policy has been amended to provide further detail of how NICE will handle information rights complaints made by data subjects who could be considered employees of NICE. |

**Annex a) Information Rights Complaints Policy & Grievance Decision Tree**



**Annex b) Information Rights Complaints Policy & Grievance Process Map**

