Data subject rights policy

Introduction

1. We are the professional regulator for nurses and midwives in the UK and nursing associates in England. Our principal functions include setting standards of education, training, conduct and performance for nurses and midwives, and ensuring the maintenance of those standards.

2. We process large amounts of personal data about a variety of people, including applicants for registration, nurses and midwives and nursing associates in England and witnesses in fitness to practise cases. The NMC is also an employer and we therefore process personal data about our staff and individuals who wish to work for us.

3. The Data Protection Act (DPA) 2018 and the UK General Data Protection Regulations (UK GDPR) sets out eight rights, which individuals can exercise in terms of their personal information. This policy sets out how we seek to enable data subjects to exercise their rights in accordance with the legislation. The legislation gives individuals the following rights:

    3.1. The right to be provided with specified information about the processing of their personal data ('**the right to be informed'**).

    3.2. The right to access their personal data and certain supplementary information ('**the right of access'**, sometimes known as 'Data Subject Access').

    3.3. The right to have their personal data rectified, if it is inaccurate or incomplete ('**the right of rectification**').

    3.4. The right to have, in certain circumstances, their personal data deleted or removed ('**the right of erasure**', sometimes knowns as '**the right to be forgotten**').

    3.5. The right, in certain circumstances, to restrict the processing of their personal data ('**the right to restrict processing**').

    3.6. The right, in certain circumstances, to move personal data the individual has provided to another organisation ('**the right of data portability**').

    3.7. The right, in certain circumstances, to object to the processing of their personal data and, potentially, require the NMC to stop processing that data ('**the right to object**').

3.8. The right, in relevant circumstances, to not be subject to decision-making based solely on automated processing (‘**Rights related to automated decision making, including profiling’**).

Aims of the policy

4. This policy sets out our commitment to:

4.1 respond to all data subject rights requests in a person centre manner and according to the values of transparency and integrity;

4.2 ensure that all personal data is processed fairly and lawfully and in accordance with data subjects' rights;

4.3 ensure that everyone working for us or on our behalf to comply with this policy when dealing with data subject rights;

4.4 identify the approach that we will routinely take when responding to requests, including setting out in general terms any exemptions in the DPA we are likely to apply when responding to requests.

Scope

5. This policy applies to all data subject rights requests that we receive.

6. Apart from requests made on behalf of data subjects by an agent acting for that data subject, this policy does not cover requests for personal data made by third parties under the Freedom of Information Act or, as a Third Party Disclosure Request where a legitimate legal basis has been cited for the release of personal information. Our approach to such requests is explained in our *Freedom of Information policy* and our *Data sharing policy* respectively.

Roles and Responsibilities

7. The Data Protection Officer will monitor compliance with this policy and provide advice on responding to data subject rights requests.

8. The Customer Information and Data Requests team is responsible for managing all responses to data subject rights requests within organisational and statutory deadlines.

9. All staff are responsible for:

9.1. Identifying data subject rights requests

9.2. Referring data subject rights requests immediately to the Customer Information and Data Requests team: foi&dparequest@nmc-uk.org

9.3. Co-operating with and assisting the Customer Information and Data Requests team to coordinate responses to requests.

10. We will provide staff with appropriate training/guidance so that they are able to comply with their responsibilities under this policy.

Policy review

11. We will review this policy every year, or more frequently in the event of any legislative or regulatory changes.

Policy statements

Details of how to make a request

12. We will publish information about how people can exercise their data subject rights on our website including details of reasonable adjustments that we can offer to ensure that these rights are accessible to all.

Confirmation of request and identity

13. The Customer Information and Data Requests team will normally ask applicants to provide written confirmation of their request via email or letter. This is because of the requirement to be satisfied of the applicant's identity and for audit purposes.

14. The team can accept data subject rights requests by telephone however, these may be subject to further identity checks. In any circumstance, we reserve the right to make identity checks as deemed necessary.

15. The team will not usually progress a subject rights request until it has received the requester's:

    15.1. full name

    15.2. previous name(s) (if applicable)

    15.3. address and/or email address

    15.4. date of birth (if the requester is a registrant)

    15.5. PIN number (if the requester is a registrant)

    15.6. case reference number (if applicable)

    15.7. authorisation to communicate with a third party (if applicable).

16. Depending on the circumstances, the team may ask the applicant (or their representative) for further proof of identity or authority to act.

17. Where the team is otherwise satisfied as to the identity of the person making the request, it may elect to waive the requirement for the applicant to provide proof of identity.

Clarifying the request

18. Where we have a large amount of information relating to the applicant or a request is unclear, the Customer Information and Data Requests team may ask the applicant to clarify what specific information that they are looking for. The team will send clarifying correspondence to the applicant as soon as possible following receipt of the request.

Timescale for compliance

19. The Customer Information and Data Requests team must log the date that request was received and the applicant's identity confirmed. The date that a request becomes active will be the date that a valid request is made (i.e. subject to clarification and identity checks).

20. The team will aim to deal with all requests promptly and to respond within one month. Where this is not possible the team must within one month tell the applicant:

    20.1. that they are extending the response time for up to two months and the reasons why, or

    20.2. why they have decided not to respond to the request and that they can complain to the ICO or seek a judicial remedy.

21. The time limit to comply is calculated from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, we have until the next working day to respond.

22. The team will monitor the time taken to comply with requests and report to the Data Protection Officer on compliance.

Multiple requests and additional copies

23. If multiple or subsequent requests are unfounded or excessive (in particular because of their repetitive character), we may either:

    23.1. Charge a reasonable fee, or

    23.2. Refuse to act on the request.

24. In deciding whether multiple requests are excessive or made at unreasonable intervals, the Customer Information and Data Requests team will take into account :

    24.1. The nature of the data, including whether it is particularly sensitive

    24.2. The purposes of the processing, including whether it is likely to cause a detriment to the applicant

24.3. The frequency with which the data is altered, including whether the data is likely to have changed or been altered since the previous request

24.4. The time that has elapsed since the previous request

24.5. The volume of information or investigation involved

24.6. Any reasons given by the applicant for wanting the same information or, making the same request again

24.7. Whether information requested under the right of access would be disclosable through other routes. We routinely disclose large volumes of personal data to registrants involved in fitness to practise proceedings. We will therefore seek to clarify with applicants whether they wish to receive such information prior to sending a copy of such information.

25. The team will keep a record of their decision-making and respond to any requests by the applicant for a review of their decision.

Searching for personal data

26. The Customer Information and Data Requests team will undertake a reasonable and proportionate search for the personal data pertaining to a request in conjunction with relevant staff.

27. A record of any search parameters and strategy used must be clearly recorded in every case.

Amending data that is the subject of a request

28. It is a criminal offence for staff to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure or accurate response to a person who has made a data subject rights request unless:

28.1. The data would have been amended in any event; and/or

28.2. We reasonably believe that the individual is not entitled to receive the requested information in line with a valid exemption under the DPA.

29. We will consider the data held at the time a request was received. However, in many cases routine use of the data may result in it being amended while the request is being dealt with. We may therefore consider the information we hold as at the date of the response, even if this is different to that held when the request was received.

30. It is however important to note that for some data subject rights requests, we sometimes need to alter or erase data to comply with the request itself, this applies to the rights of erasure and rectification.

Review of the information

31. Once the relevant information has been located, the Customer Information and Data Requests team will review the data prior to making a decision on whichever data subject right has been exercised and will decide whether any exemptions apply or, if there are legitimate reasons why we are unable to action a request.

32. With regards specifically to the right of access, the subject access right is to information (i.e. personal data) and not to documentation. Accordingly the team may extract the applicant's personal data from documentation or redact information, which is not the applicant's personal data when preparing our response. Where appropriate, the team may provide relevant contextual information to assist the applicant.

33. For complex requests the Customer Information and Data Requests Manager and/or a member of the General Counsel team will review the information prior to making a decision. In the most sensitive cases, further escalation and review may be necessary.

Exemptions

34. The DPA and UK GDPR set out a number of exemptions which may apply to data subject rights requests. We may be exempt from complying (in full or in part) with a request if:

    34.1. The information sought is classed as 'third party data' meaning that it is information about other individuals and not the requester.

    34.2. We do not have the consent to release third party information and it is not reasonable in the circumstances to disclose the data

    34.3. The disclosure of information or, granting an individual's request would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders

    34.4. The disclosure of information or, granting an individual's request would prejudice our regulatory functions, or the functions of another regulator

    34.5. The information contains legally privileged personal data

    34.6. Disclosure of information or, granting an individual's request would be likely to prejudice our negotiations with the data subject

    34.7. We are asked to erase data which we are required to process in order to comply with a legal obligation, for the performance a task carried out in the public interest or for reasons of public interest.

    34.8. There is another applicable exemption in the DPA or, UK GDPR.

Other reasons we may refuse a request

35. There are other reasons beyond the above exemptions which may result in us refusing a request in part or in full. In terms of the data subject rights of erasure, rectification, restriction of processing and, objection, there are often legitimate reasons why we are unable to action the requested outcome. We're required **by law** to publish and retain certain personal information therefore, this can result in us being unable to meet desired outcomes.

Response

36. The Customer Information and Data Requests team will usually respond to requests by email unless this is not possible or, another contact method has been specified by a requester.

37. The team will take appropriate security measures to protect the response from unauthorised disclosure in accordance with our *Information classification and handing policy.*

38. Our responses to data subject rights requests will contain the following information.

    38.1. A summary of the request

    38.2. Our decision as to disclosure or, whether we are granting or refusing a request

    38.3. Clear reasons for any redactions, exemptions or, our reasons for refusing to grant a request. We will cite relevant sections of the DPA and UK GDPR in these circumstances.

    38.4. Any information we need to send to comply with a request will be attached

    38.5. Information about how an Internal Review can be requested along with contact details for the Information Commissioners Office (ICO)

    38.6. Supplementary information about the way we process personal data

Audit and record keeping

39. The Customer Information and Data Requests Team will maintain records of:

    39.1. the requests we receive

    39.2. the 'raw' products of any searches undertaken and the strategy used

39.3. a master copy of any information about the applicant which we have collated to comply with a request along with a record of any exemptions applied

39.4. any correspondence with the applicant, including our final response

39.5. any advice received or records prepared during the course of handling the request.

Internal Reviews and the Information Commissioner's Office (ICO)

40. We will, where appropriate, voluntarily review responses that applicants are not happy with, so as to resolve any complaint or dispute in a proportionate manner, this stage is called an Internal Review.

41. Complaints about responses should be referred to the Customer Information and Data Requests Manager.

42. If the Customer Information and Data Requests Manager has been involved in making decisions on disclosure of information, the internal review will be managed by the Head of Customer Enquiries and Complaints.

43. Additionally, individuals have a right to request that the Information Commissioner make an assessment of compliance of particular circumstances with the requirements of data protection legislation.

Related policies and documents

Glossary

Data Protection Legislation	From 25 May 2018 the UK General Data Protection Regulation (UK GDPR) together with the Data Protection Act 2018 (the Data Protection Legislation) governs the processing of Personal Data. The Data Protection Legislation requires that Personal Data including Special Categories of Personal Data, which are regarded as more sensitive, must be processed by Data Controllers in accordance with the data protection principles set out in the UK GDPR.
Data Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. We are a Data Controller for the purposes of Data Protection Legislation
Data Processor	Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.
Data Subject	Any living individual who is the subject of Personal Data.
Personal Data	Personal Data' means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The above definition includes any expression of opinion about the individual and any indication of the intentions of the Data Controller (i.e. us) or any other person in respect of the individual.
Special Categories of Personal Data (formerly "sensitive personal data")	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Information about the commission of offences or criminal proceedings is also regarded as sensitive under Data Protection Legislation and we handle such information commensurately.

Processing	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.