Data subject access policy

Introduction

1. This is our Data subject access requests policy.

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

3. We process large amounts of personal data about a variety of people, such as applicants for registration, nurses and midwives on our register and witnesses in fitness to practise cases. The NMC is also an employer and we therefore processes personal data about our staff and individuals who wish to work for us.

4. Data protection legislation sets out that data subjects should in general have the right of access to their own personal data. This policy sets how we seek to enable data subjects to exercise their right of access in accordance with the data protection legislation

Aims of the policy

5. This policy aims to:

    4.1 state our commitment to responding to all data subject access requests (DSARs) in an open and honest way;

    4.2 state our commitment to ensuring that all personal data is processed fairly and lawfully and in accordance with data subjects' rights;

    4.3 state the responsibility of everyone working for us or on our behalf to comply with this policy when dealing with DSARs;

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

Scope

6. This policy applies to all DSARs that we receive.

7. 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, including tracer requests. Our approach to such requests is explained in our *Data sharing policy*.

Roles and Responsibilities

8. The Data Protection Officer will monitor compliance with this policy and provide advice on responding to DSARs.

9. The Records and Archives Team is responsible for managing all responses to DSARs within organisational and statutory deadlines.

10. Staff are responsible for:

    10.1. Being able to identify DSARs

    10.2. Referring DSARs immediately to the Records and Archives Team via foi&dparequest@nmc-uk.org

    10.3. Co-operating with and assisting the Records and Archives Team to coordinate responses to DSARs.

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

Policy review

12. 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

13. We will publish information about people can access the information we hold about them on our website.

Confirmation of identity

14. The Records and Archives team will normally ask applicants to provide written confirmation of their DSAR via email or letter. This is because of the requirement to be satisfied of the applicant's identity and for audit purposes.

15. The team will not usually progress a DSAR 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, the Records and Archives team may ask the applicant to clarify what specific information that they are looking for. The team should send clarifying correspondence to the applicant as soon as possible following receipt of the request.

Timescale for compliance

19. The Records and Archives Team must log the date that request was received and the applicant's identity confirmed.

20. The team must 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 team will monitor the time taken to comply with requests and report to the Data Protection Office on compliance.

Multiple requests and additional copies

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

    22.1. Charge a reasonable fee, or

    22.2. Refuse to act on the request.

23. In deciding whether multiple requests are excessive or made at unreasonable intervals, the Records and Archives Team will take into account :

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

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

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

    23.4. The time that has elapsed since the previous request

    23.5. The volume of information involved

    23.6. Any reasons given by the applicant for wanting the same information again

    23.7. Whether the information 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.

24. The team must 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

25. The Records and Archives Team will undertake a reasonable and proportionate search for the personal data requested by an applicant in conjunction with relevant staff.

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

Amending data that is the subject of a request

27. It is a criminal offence for staff to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure to a person who has made a DSAR unless:

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

    27.2. We reasonably believe that the individual is not entitled to receive the requested information.

28. Accordingly, where any normal or routine amendment or deletion of data is proposed following receipt of a DSAR, this should be discussed with the Data Protection Officer in conjunction with the Records and Archives Team.

29. We will aim to provide data held at the time the DSAR 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 supply the information we hold as at the date of the response, even if this is different to that held when the request was received.

Review of the information

30. Once the relevant information has been located, the Records and Archives Team will review the data prior to disclosure and will decide whether any exemptions apply.

31. 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.

32. For complex requests the Records and Archives Manager and/or a member of the Corporate Legal Services Team will review the information prior to disclosure. In the most sensitive cases, further escalation and review may be necessary.

Exemptions

33. We may be exempt from complying (in full or in part) with a DSAR if:

33.1. The information sought is mixed data, we do not have the consent of the other data subject to release the information and it is not reasonable in the circumstances to disclose the data

33.2. the disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders

33.3. the disclosure would prejudice our regulatory functions, or the functions of another regulator

33.4. the information contains legally privileged personal data

33.5. Disclosure would be likely to prejudice our negotiations with the data subject.

34. A considerable amount of personal data that we hold will be 'mixed' data relating to the applicant and a third party. For example a witness statement obtained in the course of a fitness to practise case will contain data belonging both to the author of the statement and the registrant. The Records and Archives Team will assess whether it is appropriate to seek consent in these cases before deciding whether or not to apply an exemption.

Response

35. Where we hold data about a data subject, our response must contain the following information:

35.1. the purpose of the processing

35.2. the categories of the personal data concerned

35.3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations

35.4. where possible, the expected period for which the personal data will be stored, or, if not possible, the criteria used to determine that period

35.5. the data subject's right to have inaccurate personal data rectified or erased and to request restriction or object to the processing of personal data

35.6. the right to lodge a complaint with a supervisory authority

35.7. where the personal data is not collected from the data subject, any available information as to their source

35.8. in cases of automated decision-making, including profiling, information about the reasons for the decision-making or profiling, as well as the expected consequences of such processing for the data subject

35.9. In the case of transfer of the data subject's personal data to a third country or an international organisation, the appropriate safeguards that we arranged in relation to the transfer

35.10. An explanation of whether and why any exemptions have been applied to the personal data we hold.

Sending our response

36. The Records and Archives team will usually respond to DSARs by email.

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

Audit and record keeping

37. The Records and Archives team will maintain records of:

    37.1. the requests we receive

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

    37.3. a master copy of the information containing all the personal data we hold about the applicant along with a record of any exemptions applied

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

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

Complaints

38. 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.

39. Complaints about responses should be referred to the Records and Archives Manager.

40. 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, and/or to start legal action to enforce their subject access rights.

Glossary

Data Protection Legislation	From 25 May 2018 the General Data Protection Regulation (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 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.