Data protection policy

Introduction

1 This is our Data protection policy.

2 We are a Data Controller and "Public Authority" for the purposes of data protection legislation.

3 This policy sets out how we intend to comply with data protection legislation and will handle personal data (and other sensitive information) in a way which will help us effectively to discharge our functions in the public interest, uphold registrants' and the public's confidence in us as a regulator, and ensure that we are a fair and effective employer.

4 There is a glossary of terms at the end of this policy along with links to all relevant policies and procedures referred to below.

Aims of the policy

5 This policy aims:

5.1 to state our commitment to compliance with data protection legislation and the principles of data protection;

5.2 to discharge our obligations to have in place data protection policies as part of measures to secure compliance with data protection legislation;

5.3 to provide a general appropriate policy document and an overarching appropriate policy document for processing of special categories of personal data, as may be required as part of data protection legislation;

5.4 to outline how we will work to comply with the data protection legislation through the use of technical and organisational measures and in particular the principles of data protection by design and data protection by default;

5.5 to state the responsibility of everyone working for us or on our behalf to comply with this policy and the data protection legislation;

5.6 to identify some of the circumstances where we are exempt from certain general principles because of our functions as a regulator.

Scope

6 This policy applies to all personal data as defined by the data protection legislation whether it is held by us, transferred to or exchanged with third parties, or held by third parties on behalf of us. This applies whether the data is held in electronic and paper form.

Roles and responsibilities

7 The Chief Executive and Registrar is ultimately responsible for our compliance with data protection legislation.

8 The Executive Board is responsible for maintaining this policy and may delegate responsibility for approving changes to the policy to the Information Governance and Security Board (IGSB).

9 The Data Protection Officer has the responsibilities set out in the General Data Protection Regulation.

10 There is more information about specific roles and responsibilities in the Information Security Roles and Responsibilities RACI chart.

11 Managers within every business area are responsible for implementing and ensuring compliance with data protection procedures. This includes the requirement to take all reasonable steps to ensure compliance by third parties.

12 Managers must contact the Information Assurance and Compliance team if they are unsure about what security or other measures they need to implement to protect personal data.

13 Managers must always contact the Data Protection Officer if:

13.1 they are unsure of the lawful basis which they are relying on to process personal data

13.2 they need to rely on consent for processing personal data

13.3 they need to prepare privacy notices or other transparency information

13.4 they are unsure about the retention period

13.5 they are unsure on what basis to transfer personal data outside the European Economic Area (EEA)

13.6 they are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment

13.7 they plan to use personal data for purposes other than those for which it was originally collected

13.8 they plan to carry out activities involving automated processing including profiling or automated decision-making

13.9 they plan to share data with another organisation or person in a way which is new or could affect data subjects' rights.

14 Managers must always contact the Procurement team if they require help with contracts governing data sharing with suppliers.

15 Everyone working for us or on our behalf is responsible for ensuring that they understand and follow this policy and other procedures relating to the processing and use of personal data and support us in complying with data protection legislation.

Compliance

16 Everyone working for us or on our behalf is required to comply with this policy.

17 Staff will be required to complete mandatory data protection training.

18 We will regularly review the systems and processes under our control to ensure they comply with this policy.

19 We will investigate any alleged breach of this policy. An investigation could result in us taking action up to and including dismissal; removal from office; or, termination of a contract for services.

Policy review

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

Policy statements

The data protection principles

21 The principles set out in data protection legislation require personal data to be:

21.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency)

21.2 Collected only for specified, explicit and legitimate purposes, and not further processed in a way which is incompatible with those purposes (Purpose limitation)

21.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data minimisation)

21.4 Accurate and where necessary kept up to date (Accuracy)

21.5 Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage limitation)

21.6 Processed in a way that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality)

21.7 Not transferred to another country without appropriate safeguards being in place (Transfer limitation)

21.8 Made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (data subject's rights and requests).

22 We are responsible for, and must be able to demonstrate compliance with, the data protection principles listed above (Accountability). This policy sets out below, in general terms, how we approach these issues.

Processing and use of Personal Data

23 We will maintain a general record of processing which sets how we process personal data in accordance with data protection legislation.

24 In general terms, we primarily process personal data about:

24.1 People who wish to be, are or have previously been on our register

24.2 People working for us or on behalf of us

24.3 People helping us to perform our regulatory functions, such as referrers and witnesses in fitness to practise cases

24.4 External stakeholders and customers engaging with us about the work we do, including those who wish to make a complaint about us.

25 We do not generally rely on consent to process personal data and special category personal data.

26 We generally rely on the following lawful bases for processing personal data:

26.1 the processing is necessary to perform a contract with the data subject

26.2 the processing is necessary to comply with our legal obligations

26.3 the processing is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the NMC

26.4 where not part of the performance of our functions, the processing is necessary for the purposes of legitimate interests pursued by the NMC.

27 Certain activities we carry out may not be covered by the above. In such circumstances, we will record the legal basis for processing.

28 We process certain special category personal data in connection with our functions as an employer and to perform certain regulatory obligations. For example, we investigate allegations relating to health or cautions and convictions. In general terms, the legal bases for such processing are:

28.1 It is necessary for the purposes of performing or exercising obligations or rights of the NMC or the data subject for the purposes of employment

28.2 It is necessary for the exercise of our functions as set out in our legislation and is necessary for reasons of substantial public interest

28.3 It is necessary for the purposes of promoting and maintaining equality of opportunity or treatment by the NMC

28.4 It is necessary for preventing or detecting unlawful acts, must be carried out without the consent of the data subject so as not to prejudice those purposes, and is necessary for reasons of substantial public interest

28.5 It is necessary to protect the public against dishonesty, malpractice, unfitness or incompetence, must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and is necessary for reasons of substantial public interest.

Transparency

29 General information about how we process personal data as a regulator (referred to as “fair processing information”) will be available on our website through privacy notices and other public-facing material.

30 We will communicate fair processing information to colleagues on iNet.

31 We will normally provide fair processing information we collect the personal data. If we don’t, we will provide the information within 30 days. In certain circumstances it may not be possible or appropriate to provide fair processing information within that timeframe.

32 As a regulator, we are excluded from certain obligations to provide fair processing information (and other data subject rights) if the processing would prejudice the proper exercise of our functions. Similarly, we may not make fair processing information available where personal data is processed to get legal advice, for the purpose of legal proceedings (including prospective legal proceedings), or to share information with the police or other law enforcement bodies.

Purpose limitation

33 We will ensure that we collect data only for specified, explicit and legitimate purposes. We will not go on to process data in any way that is incompatible with the original purposes.

34 Where we intend to use data for a different or incompatible purpose from that relied upon when we first obtained it we will:

34.1 have an appropriate legal basis for the new purpose

34.2 assess the privacy implications of the proposals

34.3 tell the data subject of the new purpose and our legal basis for processing.

Data minimisation

35 We will process personal data in a way that is adequate, relevant and limited to what is necessary for our purposes.

36 All personal data must be handled through corporate systems, for example TRIM, Case Management System and WISER. All emails (sent and received) will be on our Mimecast system.

37 Unnecessary copies of information must be deleted or securely destroyed.

38 Staff and contractors must only process personal data as required to carry out their role. We may monitor or audit the use of data to ensure that this happens.

Accuracy

39 We will ensure as far as possible that the data we hold is accurate and kept up to date. In some circumstances we may need to keep factually inaccurate information or an opinion which someone agrees with as part of our regulatory functions, such as where we are investigating an allegation that a person's entry on our register has been incorrectly obtained or fraudulently procured.

40 Staff and contractors are responsible for checking the accuracy of any personal data when they collect it. Staff and contractors must take all reasonable steps to destroy or update inaccurate personal data.

Storage limitation, retention and destruction

41 We will ensure that personal data is not kept in an identifiable form for longer than is necessary.

42 Because of our functions as a professional regulator, we keep some personal data for long periods of time. For example, we keep fitness to practise case files beyond the date when the case is closed. We do this in case we need to refer back to an earlier case file because of a new issue that has arisen concerning a registrant, or because we are challenged about our decision making. Details of all of our retention and disposal periods are set out in our retention schedule.

43 Staff and contractors are responsible for storing personal data in accordance with the *ICT user policy* and complying with the retention periods set out in our retention schedule.

Security, integrity and confidentiality

44 We will develop, implement and maintain appropriate data security systems to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

45 We will regularly review, evaluate and test the effectiveness of our data security systems.

46 Staff and contractors must comply with our *ICT user policy* and *Information classification and handling policy*. These policies set out the actions that must be taken to protect the 'Confidentiality', 'Integrity' and 'Availability' of all personal data from the point of collection to the point of destruction. In this context:

46.1 'Confidentiality' means only people who are authorised to know and use personal data can access it;

46.2 'Integrity' means that personal data is accurate and suitable for the purpose for which it is processed; and

46.3 'Availability' means that authorised peoples are able to access the personal data when they need it for authorised purposes.

Security incidents

47 Anyone involved in or witness to an information security incident (or suspected incident) must inform an NMC manager of the incident as soon as possible after its occurrence.

48 Information security incidents must be reported and managed in accordance with the *Information security incident reporting policy* and *Serious event policy and process*.

Transfer limitation

49 We will normally only transfer data outside the EEA where it is:

49.1 necessary to fulfil our functions as a regulator

49.2 necessary in the public interest (for instance, to fulfil the functions of a similar regulator overseas)

49.3 the data subject has explicitly consented to the transfer; or

49.4 necessary to issue or defend legal claims.

Rights and requests

50 Data subjects wishing to exercise their rights under data protection legislation should generally make their request in writing via our website so that the request can be processed by the Customer Information and Data Requests team.

51 Any member of staff or contractor who receives a request from a data subject to exercise their rights must pass the request on to the Customer Information and Data Requests team as soon as possible.

52 All subject access requests should be managed in accordance with our *Subject access request policy*.

Record keeping

53 All staff and contractors must keep and maintain accurate corporate records reflecting our processing.

Privacy by design

54 We will implement appropriate technical and organisational solutions (like pseudonymisation) to ensure compliance with data privacy by design principles.

55 Managers are responsible for assessing and implementing appropriate privacy by design solutions on all programmes, systems and operations that involve processing personal data. In doing so managers will take into account the following:

55.1 the state of the art;

55.2 the cost of implementation;

55.3 the nature, scope, context and purposes of processing; and

55.4 any adverse impact the processing may have on the rights and freedoms of data subjects.

Data protection impact assessments

56 We will consider the need for, and where appropriate go on to conduct, Data Protection Impact Assessments (DPIAs) in respect of our data processing activities.

57 We will conduct a DPIA (and discuss the findings with the Data Protection Officer) where we are undertaking a new processing activity which is likely to result in a high risk to the rights and freedoms of the data subject.

58 In particular, Directors will ensure a DPIA is carried out when proposing major system or business change programmes, or conducting reviews of such programmes, which will :

58.1 use systematic and extensive profiling or automated decision-making to make significant decisions about people

58.2 process special category data or criminal offence data on a large scale;

58.3 systematically monitor a publicly accessible place on a large scale;

58.4 use innovative technology in combination with any of the criteria in the European guidelines on DPIAs;

58.5 use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;

58.6 carry out profiling on a large scale;

58.7 process biometric or genetic data in combination with any of the criteria in the European guidelines on DPIAs;

58.8 combine, compare or match data from multiple sources;

58.9 process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines on DPIAs;

58.10 process personal data in a way that involves tracking individuals' online or offline location or behavior, in combination with any of the criteria in the European guidelines on DPIAs;

58.11 process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;

58.12 process personal data that could result in a risk of physical harm in the event of a security breach.

59 The record of the DPIA must be filed with the Data Protection Officer.

Automated processing and decision making

60 Generally, we will not engage in automated processing/profiling, or automated decision-making. Some business services are supported by rule based logic for the benefit and convenience of our registrants, for instance web-based automatic renewal systems that our registrants can use.

61 Where we engage in an automated decision making/profiling, we will inform the data subject of the reasons for the decision making or profiling and any consequences arising. We will also give the data subject the right to request human intervention, express their point of view or challenge the decision. Where possible we will do this prior to the decision being taken.

Data Processors

62 We may contract with other organisations to process personal data on our behalf.

63 We will only appoint a data processor if, having carried out due diligence, we are satisfied that they can implement appropriate technical and organisational measures that meet the requirements of the data protection legislation.

64 The appointment of a data processor must include the contractual requirements specified in data protection legislation.

Data sharing

65 Any sharing of personal data with external third parties must comply with our *Data sharing policy* and/or *Subject Access requests policy*, as relevant.

Use of monitoring and surveillance technology

66 Any use of audio recording, video recording, CCTV or other monitoring and surveillance technologies must comply with our *CCTV policy.* Where any new use of CCTV or surveillance technologies are being considered, a DPIA should be carried out.

Complaints procedure

67 Anyone who considers that this policy has not been followed may make a complaint following our complaints procedure. The Data Protection Officer will be made aware of the complaint and may be asked to advise on the response.

Glossary

Data Protection Legislation	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. The NMC is 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. the NMC) or any other person in respect of the individual.
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.
Special	Personal data revealing racial or ethnic origin, political opinions,

Categories of Personal Data (formerly "sensitive personal data")	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.
Transfer of data outside the EEA	When data is transmitted, sent, viewed or accessed in or to a country outside the EEA