The
NIGHTINGALE
Fund Council
ESTABLISHED 1857

The Nightingale Fund Council

Data Protection Policy

Last Updated	15.09.21

Definitions

NFC	Means The Nightingale Fund Council, a registered charity
Data Subjects	Means individuals whose data the charity processes
GDPR	Means the General Data Protection Regulation
Responsible person	Means The Nightingale Fund Council Vice Chair
Register of systems	Means a register of all systems or contexts in which personal data is processed by the charity

1. Introduction

This policy sets out the obligations of the Nightingale Fund Council, registered charity number 205911, regarding data protection and the rights of individuals in respect of their personal data under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), collectively known as the Data Protection Legislation.

The GDPR defines personal data as any information relating to an identified or identifiable natural person; an identifiable natural person is a living human being 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.

2. Data protection principles

The Nightingale Fund Council (NFC) is committed to processing data in accordance with its responsibilities under the GDPR and takes a data protection by design and default approach.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. General provisions

a. This policy applies to all personal data processed by NFC.
b. The Responsible Person shall take responsibility for the NFC's ongoing compliance with this policy.
c. This policy shall be reviewed triannually.
d. The NFC shall register with the Information Commissioners Office as an organisation that processes personal data.

4. The rights of data subjects

The GDPR sets out the following rights of data subjects:

a. The right to be informed (part 6)
b. The right of access (part 10)
c. The right to rectification (part 10)
d. The right to erasure (part 10)
e. The right to restrict processing (part 10)
f. The right to data portability (part 10)
g. The right to object (part 10) and
h. Rights with respect to automated decision making and profiling (part 10).

For more information, please refer to the parts of this policy indicated and the Information Commissioner's Office ("**ICO**") website at www.ico.org.uk

5. Lawful, fair and transparent processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the Data Subject.
The lawful basis for processing data by the NFC is Legitimate Interests – the data processing is necessary for the purposes of the legitimate interests pursued by the NFC in order undertake its purpose.

a. To ensure its processing of data is lawful, fair and transparent, the NFC shall maintain a Register of Systems (see part 13).
b. The Register of Systems shall be reviewed triannually.
c. If the purposes and/or processes of the NFC should change in any way, the NFC shall undertake a full review of this policy, including the legal basis for data processing, and alteration made to the Register of Systems accordingly.
d. Individuals have the right to access their personal data and any such requests made to the NFC shall be dealt with in a timely manner (see part 10).

6. Data minimisation

a. The NFC shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. The NFC collects and processes data set out in the Register of Systems detailed in part 13, and includes data collect from the Data Subject and third parties.
c. The NFC shall inform Data Subjects of data collection and the purposes for processing and retention through its privacy policy available through the website and signposting to the Privacy Policy on the grant application form.
d. The NFC only collects, processes and holds personal data for the specific purposes set out in the Register of Systems.
e. The NFC does not collect data concerning children, criminal offences or convictions, or special category data (special category data includes data concerning details of your race/ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, health information and genetic and biometric data).
f. Data Subjects are kept informed of the purposes for which the NFC uses their personal data through the NFC Privacy Policy.

7. Data accuracy

a. The NFC shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

8. Data retention and removal

The NFC only collects a minimum amount of data for the associated purpose and deletes that data promptly once it is no longer required.

a. Any soft copy of personal data is stored for a maximum of five years and erased by deletion from the computer system with the exception of candidate name and National Insurance Number which is retained for 7 years to comply with HMRC requirements.
b. Any hard copy of personal data is stored for a maximum of six months and destroyed by shredding.

9. Security

a. The NFC shall ensure that personal data is stored securely using modern software that is kept up to date.
b. Access to personal data shall be limited to NFC members.
c. Soft copy of personal data shall be kept on the cloud- based Office 365 system. Hard copy of personal data shall be kept to a minimum and stored in a locked filing cabinet.
d. All correspondence with applicants and Council members where personal data is shared shall be achieved via a cloud- based system which is password and secondary authentication protected.
e. All passwords used to protect personal data should not use words or phrases which can be easily guessed.
f. Emails shall not contain personal data in the body of the email but only in attachments to the email.
g. No personal data may be shared informally and must be handled with care at all times and not left on view to non- council members.
h. Any personal data used to evidence impact of the NFC's activities shall be anonymised.
i. The NFC shall never share personal data for marketing purposes.
j. The NFC shall only pass on personal data to third parties in the following circumstances:
    - The individual has provided explicit consent for the NFC to pass to a named third party
    - As required by law.

In the event of a breach of security leading to an accidental or unlawful destruction, loss or alteration, unauthorised disclosure of or access to personal data, the NFC shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Information Commissioner's Office. Records shall be kept of all breaches regardless of whether notification was required or not.

10. Responding to requests and objections

a. Data Subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the NFC holds about them, what it is doing with that personal data, and why.
b. Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the Data Subject shall be informed.
c. The NFC shall take reasonable steps to verify the identity of the individual making the request.
d. In certain circumstances, Data Subjects have the right to require the NFC to rectify any of their personal data that is inaccurate or incomplete.
e. Data Subjects have the right to object to data processing and request that the NFC erases the personal data it holds about them. All requests for erasure shall be complied with and the Data Subject informed of the erasure within one month of receiving the request.
f. Data Subjects may request that the NFC restricts the processing of the personal data it holds about them. Where a Data Subject objects to the NFC processing their personal data based on its legitimate interests, the NFC shall cease such processing immediately, unless it can be demonstrated that the NFC's legitimate grounds for such processing override the Data Subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
g. Data Subjects may request that the NFC transfer their personal data to another organisation. The NFC will take all reasonable steps to verify the identity of the Data Subject making the request and will only transfer the personal data via an attachment on a cloud based system to a named Data Controller in the third party organisation.
h. The NFC does not undertake automated decision making or profiling.
i. Data Subjects have the right to lodge a complaint with the Information Commissioner if they feel their rights have been infringed. However the NFC encourages Data Subjects to contact them in the first instance to be able to promptly and efficiently resolve any concerns or complaints the Data Subject may have.

11. Accountability

The NFC shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy.

a. The Responsible Person shall undertake a yearly audit to monitor adherence of the NFC with this policy.
b. The NFC shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of Data Subjects under the GDPR.

12. Training

a. The NFC shall provide all new Council members with copies of the NFC data protection and privacy policies.
b. The NFC shall provide all new Council members with a copy of the Information Commissioner's Office Guide to the General Data Protection Regulations.
c. All new council members shall be made fully aware of both their individual and the NFC's responsibilities under the Data Protection Legislation and under this policy.
d. The NFC shall monitor Council member's adherence with this Data Protection Policy and remind all Council members of their responsibilities under the GDPR yearly.

13. Register of Systems

Purpose	Data (key elements)	Data Retention Time	Those Data Shared With	Legal Basis
Enquiring about the organisation and its work	Name, email address, email message, letter,	Hard Copy six months Soft copy five years	NFC Honorary Secretary, NFC Council members and Trustees.	Legitimate interests – it is necessary for the NFC to read and store the message so that it can respond in a way the individual would expect.
Grant application and consideration	Name, email, telephone number, home address, course applied for, Nursing and Midwifery Council number, employer contact details, referee contact details, employment history, personal statement in support of application, CV, references.	Hard Copy six months Soft copy five years	NFC Honorary Secretary, NFC Council members and Trustees.	Legitimate interests – it is necessary for the NFC to read, discuss and store the application form, CV and references so that it can give full consideration to each application.
Grant awarding	As above.	Hard Copy six months Soft copy five years National Insurance Number and name only 7 years (HMRC requirement).	NFC Honorary Secretary, NFC Council members and Trustees.	Legitimate interests – it is necessary for the NFC to store the application form, CV and references so that it can respond to any queries or subsequent additional applications from the individual.

Name:	Sue Martin
Position:	Chair
Date:	Sept 2021
Due for review by:	30.09.2024