Overseas Fellowship of Nigerian Christians

GDPR Data Protection Policy

Code:	
Version:	1.0
Date of version:	14 April 2018
Created by:	GDPR implementation committee
Approved by:	National Executive Council (NEC)
Confidentiality level:	

Change history

Date	Version	Created by	Description of change

Table of Contents

1.0 Introduction

Oversees Fellowship of Nigerian Christians (OFNC) as a charity organisation is committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data for the purpose of delivering services according to our mission and objectives. These can include data on members, donors, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy sets out OFNC's commitment to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with the European Union General Data Protection Regulation 2016 (EU GDPR) and ensure that officials and volunteers understand the rules governing their use of personal data to which they have access in the course of their work.

1. 1 Interpretation

Any reference to the OFNC means the Overseas Fellowship of Nigerian Christians, (charity registered in the United Kingdom, charity no. 1126774 Or the Overseas Fellowship of Nigerian Christians LTD, company limited by guarantee, in England and Wales, Registration no. 6534207. Any reference to the NEC means the National Executive Council of the OFNC and any reference to the BEC means the Branch Executive Committee

1.2 Why this policy exists

The purpose of this policy is to set out OFNC's commitment for protecting personal data. The National Executive Council (NEC) of OFNC regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

OFNC will remain the data controller for the information held. The NEC, officials and volunteers will be personally responsible for processing and using personal information in accordance with the GDPR.

NEC, officials and volunteers who have access to personal information, will be expected to read and comply with this policy. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2.0 The Principles

OFNC shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible to comply with these principles. The Principles are:

2.0.1 Lawful, fair and transparent

We will ensure fair, lawful as well as open and transparent collection and utilisation of data.

2.0.2. Limited for its purpose

We will collect data for specific purposes in line our mission and objectives.

2.0.3. Data minimisation

We will ensure that only necessary data is collected and not excessive for its purpose.

2.0.4. Accurate

We will ensure that the data we hold is accurate and kept up to date.

2.0.5. Retention

We will ensure that data is not stored longer than necessary.

2.0.6. Integrity and confidentiality

We will ensure that the data we hold is kept safe and secure.

2.0.7. Accountability

We will ensure demonstrable compliance with the principles as listed above.

2.1 Definitions

Business purposes	The purposes for which personal data may be used by OFNC: Personnel, administrative, financial, regulatory, and business development purposes. *Business purposes include the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring business policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Marketing our business* - *Improving services*
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. *Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the 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; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means 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.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is [the Information Commissioners Office].

2.2 Policy scope

This policy applies to The Overseas Fellowship of Nigerian Christians (OFNC) and it includes:

- The head office and NEC of Trustees/directors
- All branches
- All staff and volunteers and members
- All contractors, suppliers and other people working on behalf of the Charity

It applies to all data that the organisation holds relating to identifiable individuals, even if that information technically falls outside of the EU-GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Financial information
- Special needs
- any other kind of information relating to individuals

This policy supplements other OFNC policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff as soon as ratified by the NEC.

2.2.1 Who is responsible for this policy?

As the Data Protection Officer (DPO), the National Secretary has overall responsibility for the day-to-day implementation of this policy but they may delegate all or part of this responsibility. You should contact the DPO for further information about this policy if necessary using the official OFNC contact email (info@ofnc.org.uk).

2.2.2 Accountability and transparency

To comply with data protection laws and the accountability and transparency Principle of GDPR, OFNC shall demonstrate compliance. Officials and volunteers are responsible for understanding their particular responsibilities to ensure they meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments, along with the DPO
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

2.2.3 Data protection risks

This policy helps to protect from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the organisation uses data relating to them.
- **Reputational damage.** For instance, the organisation could suffer if hackers successfully gained access to sensitive data.

2.2.4 Responsibilities

Everyone who works for or with the OFNC has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **National Executive Council (NEC)/trustees** is ultimately responsible for ensuring that OFNC meets its legal obligations.
- The National Secretary (as the DPO) is responsible for:
    - Keeping the NEC updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and/or providing advice for those covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to access data held about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the Fellowship's sensitive data.

  The National Publicity Secretary is responsible for:

    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

  The IT manager/**website administrator, (under the supervision of the** National

  Publicity Secretary) is responsible for:

    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

3.0 General guidelines for officials

- The only people able to access data covered by this policy should be those who **need it to function effectively.**
- Data **should not be shared informally**. When access to confidential information is required, members/donors can request it from the National Secretary.
- **OFNC will provide training** to all employees/officials to help them understand their responsibilities when handling data.

- Officials should keep all data secure, by taking **sensible precautions** and following the guidelines below.
    - In particular, **strong passwords must be used** and they should never be shared.
    - Personal data **should not be disclosed** to unauthorised people, either within the organisation or externally.
    - Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of (please refer to OFNC data storage policy for more details).
    - Officials **should request help** from the data protection officer (National Secretary) if they are unsure about any aspect of data protection.

4.0 Fair and lawful processing

OFNC shall process personal data fairly and lawfully in accordance with individuals' rights under the first Principle (Section 2.0.1).

If OFNC cannot apply a lawful basis, the processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

4.0.1 Controlling vs. processing data

OFNC is classified as a Data Controller and Data Processor. OFNC shall therefore maintain appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and processing data.

4.0.2 Accuracy and relevance

The law requires to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
Data will be held in **as few places as necessary**. Officials should not create any unnecessary additional data sets.
It should be **easy for data subjects to update the information** held about them. For instance, via the Fellowship's website.

4.0.3 Data security

OFNC shall keep personal data secure against loss or misuse. Where other organisations process personal data as a service on behalf of the Fellowship, the OFNC shall act in accordance with its Third-Party policy.

Personal data is of no value to OFNC unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, officials should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees and volunteers **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.
- **Data printouts should be shredded** and disposed of securely when no longer required.

4.0.4 Data collection

As much as possible, data collection shall be via electronic media such as a tablet, PC or smartphone in accordance with the data collection and storage policy.

4.0.5 Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller **(Under the supervision of the** National Publicity Secretary).

OFNC shall store and maintain a cloud-based and centralised database of all her members.

When data is **stored on paper,** it should be kept in a secure place accessible only to authorised persons.

Where data is printed in hard copies, this guideline shall apply:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Officials should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.

- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not in use.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the OFNC's standard backup procedures.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

5.0 Rights of individuals

OFNC shall respect and comply with the rights of individuals as regards to their data to the best of our ability. We shall ensure individuals can exercise their rights in the following ways:

5.0.1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

5.0.2. Right of access

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

5.0.3. Right to rectification

- OFNC shall rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done within 30 days of request but this time can be extended by another 30 days under exceptional circumstances. The data subject shall be informed of the extension.

5.0.4. Right to erasure

- OFNC shall delete or remove an individual's data if requested as detailed in Section 6.2, and if there is no compelling reason for its continued processing. The data subject will be informed when this is completed.

5.0.5. Right to restrict processing

- OFNC shall comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- OFNC is permitted to store personal data if it has been restricted, but not process it further. We shall retain enough data to ensure the right to restriction is respected in the future.

5.0.6. Right to data portability

- OFNC shall provide individuals with their data so that they can reuse it for their own purposes or across different services.
- OFNC shall provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

5.0.7. Right to object

- OFNC shall respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- OFNC shall respect the right of an individual to object to direct marketing, including profiling.
- OFNC shall respect the right of an individual to object to processing their data for scientific and historical research and statistics.

5.0.8. Rights in relation to automated decision making and profiling

- OFNC shall respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

6.0 Subject Access requests and Procedure

6.0.1 Data Portability

The DPO shall provide an individual with a copy of the information they request, free of charge in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. This shall be provided either to the individual who has requested it, or to the data controller they have requested it be sent to. This must occur without delay, and within one month of receipt. Where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month.

OFNC can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request that the individual specify the information they are requesting.

Once a subject access request has been made, OFNC shall not change or amend any of the data that has been requested before or after it has been sent.

6.0.2 Right to erasure

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a person under the age of 16 and there is no parental consent in place.

6.1 How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we shall inform them of those recipients.

6.2 The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. In such circumstances OFNC will cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

The OFNC shall inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We shall offer a way for individuals to object online.

6.3 The right to restrict automated profiling or decision making

The OFNC may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, the OFNC shall:

- Give individuals information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

7.0 Special categories of personal data

7.0.1 What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health

- sexual orientation

In most cases where OFNC processes special categories of personal data we shall require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

8.0 Privacy notices

8.0.1 When to supply a privacy notice

A privacy notice shall be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice shall be provided within a reasonable period of having obtained the data, which mean within one month.
If the data is being used to communicate with the individual, then the privacy notice shall be supplied at the latest when the first communication takes place.
If disclosure to another recipient is envisaged, then the privacy notice shall be supplied prior to the data being disclosed.

8.0.2 What to include in a privacy notice

Our Privacy notices shall be concise, transparent, intelligible and easily accessible. They are provided free of charge and as much as practical shall be written in clear and plain language.

The following information shall be included in OFNC's Privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures

- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

9.0 Disclosing data for other reasons

In certain circumstances, EU-GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the OFNC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the NEC and from the company's legal advisers where necessary.

10.0 Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. OFNC has a legal obligation to report any data breaches to Charity Commission within 72 hours.

All OFNC officials and volunteers have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Charity Commission of any compliance failures that are material either in their own right or as part of a pattern of failures

Any OFNC official or volunteer who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action. Please refer to the OFNC Data Breach Reporting procedure for details.

11.0 Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both volunteers and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action as will be determined by the NEC.

Any questions or concerns about any aspect of this policy may be directed to the DPO using the email address dpo@ofnc.org.uk