Free West Papua Campaign Data Protection Policy

1. General

This policy outlines the Free West Papua Campaign's commitments to respect the privacy of people's personal information and observe the relevant data protection legislation. It is designed to enable Free West Papua Campaign staff and others to be clear on what our data protection principles, commitments, and operating practices are. It is supported by other related guidelines and documentation.

The Free West Papua Campaign holds and processes personal data on past, current, and prospective board members, staff, volunteers, donors, individuals, and organisations we work with; and suppliers and others with whom we communicate.

The Free West Papua Campaign regards the lawful and correct treatment of personal information as crucial to our successful operations. This involves taking precautions against physical loss or damage and ensuring that access and disclosure are restricted. All staff are responsible for ensuring that:

- Personal data is only retained when necessary, and for valid reasons,
- Any personal data held is kept securely, and
- Personal information such as mobile phone numbers, social media 'handles' (online names), or email addresses, are not disclosed to any unauthorised third party, without the subject's consent.

In relation to GDPR, the Free West Papua Campaign is both a data controller and data processor. In addition, we also use third-party providers and platforms in the course of our work and operations. These are detailed below and in our Privacy Policy.

2. Principles

The Free West Papua Campaign fully endorses and adheres to the principles of the UK Data Protection Act, 1998, the EU GDPR[1], and the anticipated UK Data Protection Act, 2018. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transporting, and storing personal data. Staff, volunteers, or any other people or organisations associated or working with the Free West Papua Campaign who obtain, handle, process, transport, and store personal data for the Free West Papua Campaign must adhere to these principles.

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;
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.

[1] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/principles/

Article 5(2) requires that

"The controller [i.e. the Free West Papua Campaign] shall be responsible for, and be able to demonstrate, compliance with the principles."

- **Lawful processing**

Personal data must be processed lawfully. Under article 6 of the GDPR, a lawful basis for processing must be identified and documented before personal data can be processed. The lawful bases available are:

a) Consent of the data subject [the person whose data is stored],
b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
c) Processing is necessary for compliance with a legal obligation,
d) Processing is necessary to protect the vital interests of the data subject or another person,
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and
f) Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

- **Special category data**

Some types of personal data are considered more sensitive and need additional protection. These include personal data revealing:

a) Racial or ethnic origin,
b) Political opinions,
c) Religious or philosophical beliefs,
d) Trade union membership,
e) Genetic data,
f) Biometric data (for ID purposes),
g) Health,
h) Sex life, and
i) Sexual orientation.

These special categories of data can only be processed if one of the following applies (Article 9(2)):

a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes[…];

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection […];

c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) Processing relates to personal data which are manifestly made public by the data subject;

f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) Processing is necessary for reasons of substantial public interest, […] which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services […] or pursuant to contract with a health professional and subject to the

conditions and safeguards referred to in paragraph 3;

i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, […] which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) […] which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

- **Individual rights**

Individuals have specific rights in relation to their personal data under GDPR:

a) The right to be informed,
b) The right of access,
c) The right to rectification,
d) The right to erasure,
e) The right to restrict processing,
f) The right to data portability,
g) The right to object, and
h) Rights in relation to automated decision making and profiling.

3. Satisfaction of principles and compliance with the regulations

In order to meet the requirements of the principles, The Free West Papua Campaign has in place appropriate management controls and uses strict criteria to:

- Observe fully the conditions regarding the lawful and fair collection and use of personal data,
- Meet its obligations to specify the purposes for which personal data is used,
- Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements,
- Ensure the quality and accuracy of personal data held to the best of the Free West Papua Campaign's ability,
- Apply strict checks to determine the length of time personal data is held,
- Ensure that the rights of individuals about whom the personal data is held can be fully exercised,
- Take the appropriate technical and organisational security measures to safeguard personal data, and
- Ensure that personal data is not transferred outside the EEA and designated 'adequate protection' countries, without suitable safeguards

As identified under the Data Protection Act, the Free West Papua Campaign holds personal data for the following six purposes:

- Realising the objectives of the Free West Papua Campaign,
- Staff administration,
- Advertising, marketing, and public relations,
- Accounts and records,
- Administration of membership records, and
- Fundraising.

The section below lists the sets of personal data that the Free West Papua Campaign stores and details how the use of the data is in accordance with the legislation. The use of the data in all cases is in order to realise the aims of the Free West Papua Campaign.

5 Applying the policy

Any breach of this policy will be taken seriously and may result in disciplinary action, up to and including dismissal. Any

questions or concerns about the interpretation or operation of this policy should be raised with the Board.

Every staff member, volunteer, or consultant working for the Free West Papua Campaign is expected to adhere to the policy at all times. Any staff member or volunteer who believes that the policy has not been followed in respect of their own personal data or that of others should raise the matter with their line manager or with the Board.

Each database or file storage system has a designated person responsible for the implementation of the Data Protection Policy in relation to that particular system. Members of staff who wish to use the data may do so only with the authority of the person responsible for the particular database or system, who will ensure compliance with this policy.

The persons responsible for each database or set of personal information is as follows:

- Contacts and Fundraising Database – Digital Fundraising Officer
- Shared files and group-restricted server files – Office Administrator
- Website e-newsletter – Campaign Coordinator
- Online donations – Digital Fundraising Manager
- Recruitment – Office Administrator
- Personnel – Office Administrator
- Payroll – Office Administrator

- **Requests for access to or deletion of personal information**

Any request from a person asking to see their personal data held by the Free West Papua Campaign, have their details amended, be removed from a mailing list or database, or any other related enquiry, should be sent to the Office Administrator, who is responsible for ensuring any request is completed, actioned, or enquiry responded to. It is helpful if such requests and enquiries are also copied to the relevant person named above, to facilitate swift processing.

Any enquiries will be responded to in accordance with GDPR. Compliance with requests for data to be erased may be restricted by Free West Papua Campaign duties under other legislation, such as requirements to keep financial or employment records for tax purposes.

The Free West Papua Campaign aims to comply with requests for access to personal information as quickly as possible and will ensure that a response is provided within 30 days of receipt of a request.

If a data subject asks the Free West Papua Campaign to delete their personal data, clarification should be sought on the following:

- Would they like all their personal data to be deleted, or would they prefer that the Free West Papua Campaign keep their name and other identifying data in order to apply a 'do not contact' note? If the former, they may be re-added to the Free West Papua Campaign systems in the absence of information to the contrary, if a legitimate interest is subsequently established.
- Do they wish their personal data to be deleted from backups or is it acceptable to delete their data only from live systems? If the former, please see 'retention of data' below.

6. Free West Papua Campaign databases and IT systems

The Free West Papua Campaign maintains a number of internal systems for the storage and use of individuals' contact details and other personal data. The people who have overall responsibility for each of these are listed above.

When using any of these systems for the storing of personal data, it is the individual staff member's responsibility to ensure that they undertake the following:

- Determine a legal basis for storing/processing the personal data,
- As part of the Free West Papua Campaign's automated workflow, ensure the provision of any privacy notices required to the data subjects whose personal data is being processed,

- Ensure the necessary security measures are taken (e.g. password-protecting files),
- Keep the personal data up to date and accurate, and
- Undertake regular reviews of the data with a checklist, assign a new legal basis if necessary and delete when no longer needed.

- **Contacts and Fundraising Database**

For its own activities the Free West Papua Campaign maintains a database of contact information about individuals and organisations who we work with. This is password-protected and only accessible to Free West Papua Campaign staff, including volunteers and consultants, where this is necessary for their work on behalf of the Free West Papua Campaign.

- The information on this database may include a person's name, address, email address, telephone/fax number(s), job title and employer, work-related interests, plus details of their involvement with the Free West Papua Campaign including funding given, events attended, and the relationship of the individual to the Free West Papua Campaign (e.g. a mediator in a conflict or programme partner).
- Professional and other contacts are added to this database, using information from a business card or other exchange of contact details that Free West Papua Campaign staff have received during business contact with the individual.
- If staff are passed the contact details of an individual by a third party in the course of their work, they should contact the individual within one month of receiving the details, providing the relevant privacy notices. Only then, if no reason to the contrary, can they be added to the Contacts Database (using the consent or legitimate interest legal basis – see below).
- The legal basis for processing the personal data on this database must be assessed for each process. For professional contacts stored on the contacts database, the legal basis may be legitimate interest. If so, this must be reassessed if circumstances change (e.g. the end of a common project).
- Contacts deemed to be kept on legitimate interest grounds will be reviewed at least every three years without recorded contact. See the Legal Basis Guide for more information.
- If a legitimate interest cannot be established, data must be deleted or consent must be sought as follows.
    - Free West Papua Campaign staff must seek the consent of the individual to add their details to the database before doing so.
    - This consent may be verbal or written, but must indicate that they have understood the purpose of our holding their data.
    - A comment must be made on their Contacts Database record to indicate what consent was given, when and by what means.
    - Contact details from this database will only be used to get in touch for specific, relevant work purposes and will not be used to send unsolicited mass communications, such as newsletters. In order to receive such communications, individuals must subscribe to our e-newsletters via the Free West Papua Campaign website.
- Staff must not add or keep personal data that may be defamatory, inappropriate, or unnecessary for the purposes for which the data is kept.
- Staff must not add to the Contacts Database sensitive personal data ('special category data'[2] – see above) other than with the explicit consent of the data subject to process the data for a specific purpose; for example, to arrange focus groups of LGBT people or a particular religious group.
- Individuals may directly ask for their data to be removed from any of the Free West Papua Campaign databases as described above. Where data are kept with the consent of the data subject, the Free West Papua Campaign will seek to renew this consent after four years without any recorded contact. Data will be removed if consent is sought and not given.
- All individual contacts will have a staff member or team assigned to them, and those staff are responsible for ensuring that the personal data and other information for that contact is kept up to date.
- Data will be removed when they are believed to be out of date or no longer necessary for the work of the Free West Papua Campaign.

- **Shared files and group-restricted server files**

The Free West Papua Campaign maintains a system of 'shared files' on its server and cloud storage where various documents are stored for each team in the course of their work. This may include documents that contain personal data. Only staff with a system's login, consultant and volunteers (when necessary for their work), and contracted IT staff, are able to access these folders and files.

- Documents on Shared files containing personal data are likely to take the form of lists of activity participants and event invitees, lists of approved suppliers and donor reporting documents, however other types of documents may also be

[2] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

stored.

- Staff must only keep documents containing personal data on shared files for as long as is necessary for the duration of a project, fulfilment of a legal /contractual obligation or another purpose.
- Any documents stored on shared files that contain personal data should be password protected.
- The storing of personal data on documents on Shared files is likely to come under legitimate interest as a legal basis but this will need to be assessed and documented on a case-by-case basis.
- Explicit and documented consent is required from the data subject to store any 'special category' data.

- **Website e-newsletter**

The Free West Papua Campaign sends mass emails about its news and latest work via a third-party e-newsletter system, currently Keela.

- Users indicate their preferences to receive these emails by actively subscribing via the Free West Papua Campaign website, giving their consent for data to be processed. A privacy notice with a link to Free West Papua Campaign's full Privacy Policy is supplied to users at the time of subscription and is available to them at all times.
- Users subscribe via a double opt-in process.
- Users' preferences are stored in the Keela database. All recipients are given the opportunity to opt-out of these communications at any time via an 'unsubscribe' link contained in every e-newsletter.
- Individuals may ask the Free West Papua Campaign directly for their details to be removed from Keela or use the unsubscribe link in any e-newsletter to withdraw their consent.

To find out more about how Keela manages data, visit https://keela.zendesk.com/hc/en-us/articles/360001105791-Networks-for-Change-Inc-Keela-Privacy-Policy

- **Online donations**

Donations which the Free West Papua Campaign receives online are processed by a third-party provider, PayPal.

- PayPal collects the personal details of donors (name, email, and payment details) and then processes the donations on the Free West Papua Campaign's behalf.
- PayPal stores all donor details and, where this has been provided to PayPal by the donor, provides us with the names, emails and donation amounts of individuals who make online donations via a secure online platform. They do not share payment details with the Free West Papua Campaign.
- These donor details are transferred into our fundraising database Keela.
- As an EU-based organisation, PayPal are subject to EU data protection regulations. For more details of how PayPal manages personal information visit: https://www.paypal.com/en/webapps/mpp/ua/privacy-full#1

- **Recruitment**

The Free West Papua Campaign gathers personal data for the purpose of staff recruitment. Data obtained through recruitment are not used for any other purpose. This data is processed as detailed below:

- Only relevant personal information is gathered through the application form, and candidates are informed that the personal information obtained through the form will be used according to this policy.
- Applicants are informed if any of the data they supply is to be checked with a third party.
- Information is kept securely and not disclosed to a third party except those involved in that particular recruitment process.
- Staff involved in recruitment are aware of data protection regulations and are required to handle personal information with sensitivity and in accordance with the regulations.
- Identifiable personal data of applicants who are not shortlisted is not available to staff members outside the administration department.
- Application forms of unsuccessful short-listed candidates, all score sheets, and interview notes must be passed on to the office administrator who will keep them securely for a period of twelve months from the position being filled and then destroy them.
- Electronic versions of application forms of unsuccessful short-listed candidates are also deleted after twelve months of the position being filled.

- **Personnel and payroll**

Personal information about staff, consultants, volunteers, and board members is processed primarily for statutory Human Resources purposes. Staff data is kept securely on both a third-party cloud-based platform, Xero, and in documents stored securely in Dropbox.

- Such information includes (where applicable) contact details, next of kin details, bank account details for salary payment, time taken off for sickness, leave, and similar details.
- All personal information about staff which is held on the Xero system is only accessible to the Human Resources team, the individual's direct line manager and any other staff as identified in other policies and procedures, where it is necessary in order for the Free West Papua Campaign to carry out its duties as an employer. This information is available to third parties only where necessary for the Free West Papua Campaign to carry out its duties (e.g. Xero system provider, insurance company, and bank for salary payments).
- All personal information held on Free West Papua Campaign personnel records, whether maintained electronically or on paper, is only accessible to the Human Resources team and any other staff as identified in other policies and procedures, where it is necessary in order for the Free West Papua Campaign to carry out its duties as an employer.
- Work-based contact details (work telephone numbers and email address) for staff, consultants, volunteers, and board members, are available to other staff, consultants, volunteers, and board members to enable them to carry out their work. This data is available through internal email directories.
- At the point that a staff member, consultant, or volunteer leaves the Free West Papua Campaign, they may choose to give consent to their personal contact information being added to the Contacts Database. Consent must be recorded as detailed above (see 'Contacts Database').
- Basic contact information (i.e. address) is required until at least the end of the financial year in order to send P60s or other pay or tax details to former staff.
- Sensitive personal data ('special category data'), is collected with explicit consent, and used only for essential purposes such as for travel and insurance purposes.
- Staff leaving the Free West Papua Campaign are subject to the confidentiality clause in their employment contract whereby they are prohibited from disclosing any confidential information to which they may have had access during their employment at the Free West Papua Campaign.

For more information about the security measures taken by Xero visit: https://www.xero.com/uk/why-xero/benefits/security/

7. Data security

All Free West Papua Campaign staff, consultants, and volunteers must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, additional specific data security arrangements will be established and implemented in contracts with those third-party organisations. Some of the main third-party providers we currently use and share personal data with are identified above.

Personal data must not be shared with any individual or organisation outside of the Free West Papua Campaign without the explicit consent of the data subject or another documented legal basis.

- **Storing data securely**

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords and, where possible, two-factor authentication. We encourage all staff to use a password manager to create and store their passwords.
- All Free West Papua Campaign computers must lock their screens when left idle for five minutes, requiring a password to unlock.
- For each Free West Papua Campaign IT system, each user must have a separate account with a distinct password so that users' access can be permitted or restricted on an individual basis as appropriate for their work.
- Free West Papua Campaign laptop/portable computers, mobile phones, and tablets must be encrypted.
- Android and iOS devices are automatically encrypted when a lock is enabled: locks must be secure pin codes, patterns, or passwords and must activate within five minutes of 'idle' time.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used. Discs or memory sticks that hold personal data or other confidential data must be encrypted.
- If a staff member, consultant, or volunteer uses equipment that does not belong to the Free West Papua Campaign to carry out work for the Free West Papua Campaign they must ensure that it meets the same security requirements as Free West Papua Campaign equipment.
    - Laptops must be encrypted and appropriate recovery arrangements should be put in place, equivalent to

Free West Papua Campaign's key.
    - Each user of the computer or device must have a separate account with a distinct password, so that other users of the computer cannot access Free West Papua Campaign data.
- The board of directors must approve any cloud or other external system used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space. Free West Papua Campaign onsite servers are kept in a secure room, which is locked with a key and alarmed.
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

If staff are unsure about any aspect of data security, they should seek the guidance of the board of directors.

8. Transferring data internationally

There are restrictions on international transfers of personal data. Personal data must not be transferred anywhere outside the EEA, or outside approved 'adequate protection' countries' without first consulting the relevant line manager and the board of directors.

Any third-party providers we share data with who are based outside the EEA and that are not approved 'adequate protection' countries, are carefully selected to ensure they have adequate safeguards in place.

9. Access to data

Staff, volunteers, and other subjects of personal data held by the Free West Papua Campaign have the right to access any personal data that is being kept about them in electronic form, and paper-based data held in physical filing systems. Data subjects also have the right to request correction of their data, opt-out of certain processing of their data, and to have their data deleted. Except when any of these rights are superseded by legal or contractual obligations. See the above section on 'Principles'.

Any person who wishes to exercise one of these rights should contact office@freewestpapua.org. The request for access to their data should be made in writing. The Free West Papua Campaign reserves the right to charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The Free West Papua Campaign may also charge a fee to comply with requests for further copies of the same information. If personal details are inaccurate, they will be amended upon receipt of a written request detailing the inaccuracies along with the correct information. All requests will be responded to within 30 days of receipt.

The computer systems and all information held on them remain Free West Papua Campaign property at all times. With express authorisation from the email account holder or another authorised member of staff, files, telephone messages, or email account of another user may be accessed. Computer hard drives and online or server accounts may also be accessed by IT staff for maintenance, security, and administration purposes.

10. Retention of Data

The Free West Papua Campaign will keep some forms of information for longer than others. As part of our Risk Management Strategy, the Free West Papua Campaign carries out regular backups of data held on its internal databases and of all files held on its servers. The backups are either done externally or on our servers on a regular basis and at any point in time, data that is up to two years old can be retrieved. Only the office administrator and designated IT staff have access to the old data. In the event that data is restored from the backup, the staff member carrying out the procedure must be sensitive to the data protection implications of this action.

In the event of a request from a data subject for the Free West Papua Campaign to delete their personal data, if the data subject requires their data to be removed from backups, the following steps should be taken:

- Restore the most recent backup to a secure environment.
- Delete the personal data relating to that data subject.
- Back up the secure environment, labelling that backup with the date of the original backup, and a note that personal data has been deleted due to a request under the right to erasure.

- Delete the restored environment unless there is reason to keep it 'live'.
- Repeat with the next most recent backup until all backups have had the personal data removed.

11. Privacy notices

In order to fulfil the right of individuals to transparency and to fulfil our obligations under data protection legislation, we provide privacy notices to data subjects whose personal data we process. As well as a full Privacy Policy which is available on our website, we also provide separate privacy notices in different formats to data subjects at the point of collecting their data, including when people sign-up to receive our e-newsletters. In addition, we provide privacy statements to staff, consultants, and volunteers.

In addition, we include the following privacy information:

- **Email sent from a Free West Papua Campaign email address (footer):**

This email is intended only for the named addressee(s) and may contain confidential and/or privileged material. If you have received this email in error, please notify the Free West Papua Campaign immediately using office@freewestpapua.org and delete the message.

- **E-newsletters (Keela system):**

You are receiving this email because you subscribed via the Free West Papua Campaign's *website https://www.freewestpapua.org/) to receive such mailings.*

The above statement appears next to an 'unsubscribe from this list' option and an 'update subscription preferences' option, where users can decide on which types of mailings they want to receive, e.g region-specific or job opportunities.

12. Training

All staff, volunteers, and board members receive training on our Data Protection Policy and related policies. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policies and procedures.

Training is provided through a compulsory in-house seminar, as well as documented guidelines and ad-hoc support. This training and guidance covers:

- The law relating to data protection, and
- Our data protection and related policies and procedures.

13. Contact

If you have any queries about this or related policies, please contact our office at office@freewestpapua.org and your enquiry will be handled by a relevant member of staff or the board.

July 2018