Data protection Policy

Table of Contents

Section 1: Overview

1.1 Purpose

1.1.1 This Data Protection Policy (“the Policy”) regulates the way in which Frontline (“we”) obtains, uses, holds, transfers and otherwise processes Personal Data about individuals and ensures all of its employees know the rules for protecting Personal Data. Further, it describes individuals' rights in relation to Frontline’s processing of their Personal Data.

1.1.2 Frontline abides by UK data protection and privacy laws, including the Data Protection Act 2018 and the General Data Protection Regulations (“the GDPR”), in its handling of Personal Data.

1.1.3 We aim to ensure our employees are acting in accordance with these laws and the relevant regulatory guidance and any available best practice. Those requirements, together with this policy, ensure that all employees of Frontline fully understand Frontline’s obligations to comply with the DPA, GDPR and other privacy laws and regulations of the UK.

1.2 Scope

1.2.1 This policy applies to all staff who process Personal Data on behalf of Frontline in accordance with this policy (“you”).

1.2.2 This policy is available on Frontline’s fewer better rules book and can be circulate upon request to the Legal &Compliance Manager (“L&C Manager”).

1.3 Responsibilities

1.3.1 This policy is owned by the L&C MANAGER who's role it is to ensure the policy is kept up to date with relevant legislation. The L&C MANAGER will also ensure Frontline staff are aware of the latest version of the policy and have access to it.

1.3.2 All staff are responsible for complying with and making use of the policies contained herein.

1.4 Definitions

Personal data	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.
Special categories of personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health (physical and mental) or data concerning a natural person's sex life or sexual orientation.
Data controller	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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Individual/Data Subject	The person whose personal information is being held or processed by Frontline e.g applicants and participants in Programmes, staff members and volunteers.
Data subject	Any living individual who is the subject of personal data held by an organisation.
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.
Personal data	A breach of security leading to the accidental, or unlawful, destruction,

breach	loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.
Data subject consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.
DPA	Means the Data Protection Act 2018
GDPR	Means the General Data Protection Regulation (EU) 2016/679 as enacted in UK law and tailored by the Data Protection Act 2018 (UK GDPR)

Section 2: Policy and procedures

2.2 Personal data

2.2.1 “Personal Data” is defined in Article 4 of GDPR as any information (for example, a person’s name) or combination of information about a living person which allows that living person to be identified from that information (for example a first name and an address). Personal Data can also include an online identifier or one or more factors specific to the physiological, genetic, mental, economic, cultural or social identity of an individual.

2.2.2 Examples of Personal Data which may be used by Frontline programmes in its day to day business include names, addresses (e-mail and postal addresses), telephone numbers and other contact details, educational background and qualifications, health and criminal offences. It also includes staff recruitment, staff performance reviews, payroll and salary information. The definition also includes opinions, appraisals or intent regarding individuals (e.g. Frontline participants, CSWs, Firstline leaders, Fellows, staff, job applicants and individual members of the public).

2.2.3 The laws governing how we can use Personal Data apply whether the Personal Data is stored electronically (for example, in e-mails, on IT systems, as part of a database or in a word processed document) or in structured manual records (for example, in paper files or filing cabinets).

2.3 Data Processing Activity

2.3.1 Frontline is defined as a Data Controller under the GDPR. Frontline as a Data Controller collects and processes Personal Data on its staff, programme applicants, participants, Firstline leaders, fellows, subscribers, donors and others for multiple purposes, including:

a. Attraction and selection of individuals to its programmes
b. Staff recruitment
c. Maintenance of the participant/leader record
d. Employee performance management and professional development;
e. Payroll and accounting;
f. Building and managing external relationships;
g. Research and development;
h. Planning and delivering of education and training;
i. Staff and participant support and facilities management;
j. Knowledge management;
k. Health, safety and security; and
l. Other purposes required by law or regulation.

2.3.2 When we collect, record, store, use, adapt, share or erase Personal Data for any of these purposes, this is called processing, including if it is carried out by automated means. If you read, amend, copy, print, delete or send Personal Data to another legal entity (i.e. outside Frontline) this is a type of “processing” and is subject to the guidelines set out in this Policy.

2.4 Data Protection Enforcement

2.4.1 Within the UK, Data protection laws are enforced by the Information Commissioner’s Office (“the ICO”). The ICO can investigate complaints, audit Frontline’s processing of Personal Data and can take action against Frontline (and you personally in some cases) for breach of the DPA, GDPR and other relevant privacy laws. Such action may include fines or permanently or temporarily limiting processing, warnings and reprimands. Additionally, organisations which are found to be in breach of the DPA, GDPR and other privacy laws also often receive negative publicity for the breaches which can affect the reputation of Frontline as a whole.

2.4.2 Each Frontline staff member or Third Party is required to read and comply at all times with this Policy. In this Policy a “Third Party” is anyone who is not an employee of Frontline, for example agents, external organisations, consultants, contractors, and service providers who process Personal Data on behalf of Frontline.

2.5 Data Security

2.5.1 As a Data Controller, Frontline has a responsibility under Article 24 of the GDPR, to ensure that there are appropriate technical and organisational measures in place to ensure that all data processing is performed in accordance with data protection law. Frontline must keep all Personal Data (including Special Category Data – see clause 2.7) secure. This means that the Personal Data must be protected against being accessed by other companies or individuals (for example, via hacking), from being corrupted or being lost or stolen. The Personal Data must also be protected so the wrong people cannot read or use the details. This applies to details in IT systems, e-mails and attachments and paper files. This is why, for example, you have a password and controlled access rights to IT systems. You must comply with Frontline's security procedures whenever you handle Personal Data. Frontline relies on you to keep data secure and for data security and to comply with Frontline's Information Security Policy.

2.5.2 If you work away from Frontline's premises, you must comply with any additional procedures and guidelines issued by Frontline for home working and/or offsite working particularly, as this presents a potentially greater risk of loss, theft or damage to Personal Data. You must read these procedures and guidelines before processing any Personal Data away from Frontline premises.

2.5.3 Extra care is needed to secure Special Category Data because more damage is likely if it is lost. For example, if details of an individual participant's medical conditions or criminal offences data was lost or made public by mistake it would be very distressing for that individual. Be especially careful if you want to send Special Category Data to another person, including by email, that it is sufficiently secure and can only be received and accessed by the intended recipient. If in doubt, seek guidance from the Information Security Manual or from the L&C MANAGER.

2.5.4 Do not store Personal Data of any kind onto unencrypted laptops, mobile telephones, flash drives or any other storage device.

2.5.5 Frontline also recognises that adequate security is important where it arranges for outside service providers to process Personal Data on its behalf. Where such arrangements are established by Frontline, service providers must be bound by written contracts to protect the Personal Data provided to them.

2.6 Records of Processing

2.6.1 Under the GDPR organisations must maintain records of their processing activities. This is to replace the previous registration with the ICO. The following information will be recorded:

a. Name and details of Frontline and the person in charge of data protection.
b. Purposes of processing
c. Descriptions of the categories of individuals and categories of Personal Data.
d. Categories of recipients of Personal Data
e. Details of transfers to outside the EEA including documentation of the transfer mechanism safeguards in place.
f. Retention schedules
g. Description of technical and organisational security measures.

2.6.2 We may be required to make these records available to relevant supervisory authorities for purposes of investigation.

2.6.3 If you change data processing activities or begin carrying out new data processing activities, contact the LCM immediately to discuss the details in case any processing description needs to be updated.

2.6.4 It may in some cases be possible to convert Personal Data into anonymous Personal Data or pseudonymised data, such as aggregated statistical data where data subjects cannot be identified, or to use it for research provided its use will not impact or affect any data subject individually. However, it may be necessary to have warned data subjects in advance that this might happen, to explain any research and in some cases to obtain their consent. Please speak to the L&C MANAGER if you wish to convert Personal Data into anonymous or pseudonymised data or use it for research before doing so, or if you have any concerns about current use.

2.7 Lawfulness of Processing Data

2.7.1 One of the main data protection obligations requires Frontline (and its employees) to process Personal data lawfully, fairly and in a transparent manner. This means under Article 6 of the GDPR that Frontline (and each employee) must comply with at least one of the following conditions when processing Personal Data:

a. processing is necessary for the purposes of the legitimate interests pursued by the controller

b. the individual to whom the Personal Data relates has consented to the processing;
c. the processing is necessary for the performance of a contract between Frontline and the individual;
d. the processing is necessary to comply with a legal obligation placed on Frontline;
e. the processing is necessary to protect a vital interest of the individual or another person;
f. the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Frontline.

2.7.2 The individual's consent to processing Personal Data should only be relied upon where there is no other lawful basis to process data. Consent should not be assumed to be the best lawful means as in many cases a different one can be applicable. If consent is used, additional stringent conditions apply. You must discuss with the Data Protection Officer the lawful basis to be used and if consent is used to check the consent process follows the conditions.

2.7.3 Article 4 of the GDPR also defines the principles relating to the processing of Personal Data:

a. Personal Data should only be collected for specific, explicit and legitimate purposes. It should not be further processed in a manner which is incompatible with the stated purposes.
b. The Personal Data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
c. Personal Data must be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that are inaccurate are erased or rectified without delay.
d. Personal Data must not be kept for longer than is necessary for the purposes for which it is processed. Contact the L&C MANAGER if you have any concerns about data retention.

2.7.4 If in any doubt about the lawful, fair and transparent use of Personal Data, you should contact the LCM.

2.7.5 If you want to make a new use of any Personal Data held by Frontline, you must not do so unless that new use satisfies one of the lawful reasons for processing and it is described in the relevant privacy notice provided to an individual (see below). For example if someone provides their Personal Data for applying to the Frontline Programme, you may not be able to start sending them marketing e-mails unless that is covered in an appropriate privacy notice and accompanied by explicit consent from

that individual. Official guidance from the Information Commissioner's Office (ICO) states that marketing communications is nearly always reliant on 'consent' for lawful processing so this should always be considered in relation to any bulk email (e.g. newsletters and other similar communications).

2.8 Special Category Data

2.8.1 Special Category Data is Personal Data about a person's race or ethnicity, their health, their sex life or sexual orientation, their religious or philosophical beliefs, their political views or trade union membership, their physical or mental health or condition, genetic or biometric data.

2.8.2 Processing of Special Category Data is prohibited unless the processing is lawful under the categories described above and one of the following applies:

a. The individual has given explicit consent to the processing for one or more specified purposes;
b. The processing is necessary for the purposes of carrying out obligations or specific rights of Frontline in relation to employment, social security and social protection law;
c. The processing is necessary to protect the vital interests of the individual or another whether the individual is incapable of giving consent;
d. The processing related to Personal Data which has been made public by the individual;
e. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
f. Processing is necessary for reasons of substantial public interest
g. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of working capacity of the individual, medical diagnosis, provision of health or social care treatment or the management of health or social care systems and services;
h. Processing is necessary for reasons of public interest in the area of public health;
i. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

2.8.3 Special Categories Data on staff or programme participants should not be collected or otherwise processed unless it is essential to do so. Extra care must be taken with it (in addition to the normal rules for Personal Data) and it must be kept or transferred more securely. There are also additional restrictions to above in relation to criminal offences data and advice should be sought from the L&C MANAGER before collecting and processing this type of data.

2.8.4 Frontline does not generally seek to obtain Special Category Data unless:

a. The individual concerned consents that Frontline may do so, on the basis of a full understanding of why Frontline is collecting the data; or
b. Frontline's HR department needs to do so to meet its obligations or exercise its rights under employment law; or
c. In exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned or staff, participants or visitors.

2.8.5 Special Category Data should not be processed for any new purposes without the involvement of and approval from the L&C Manager In most cases new consent would be required for new purposes.

2.9 Privacy Statements

2.9.1 If Frontline is collecting Personal Data from individuals then it must at the time of collection, provide them with certain information in a privacy statement.

2.9.2 In accordance with Article 5 of the GDPR, any processing of Personal Data must be undertaken lawfully, in a fair and transparent manner. In accordance with Article 13, Frontline must provide the data subject with a privacy statement and provide certain information within that notice including:

a. Name and contact details of Frontline's Data Protection Officer (or person with this responsibility, being the joint responsibility of the Legal and Compliance Manager and Officer in this case),
b. The purpose and legal basis for processing the data,
c. Any disclosure or sharing with third parties,
d. Whether it will be transferred out of the EEA

2.9.3 Frontline must also provide the individual with information on the period for which the Personal Data will be stored, the individual's rights on rectification, erasure and data portability, whether automated decision making or profiling will be carried out and the right to withdraw consent to processing if that is relied upon as the lawful basis for processing.

2.9.4 You should therefore check whether there is an applicable privacy statement which covers the processing you intend to carry out for Frontline.

2.9.5 Personal Data should not be collected for one purpose and then used for another unless that is also set out in the relevant privacy statement.

2.9.6 If you have any questions about privacy notices, or wish to undertake a new project which involves a change in the way individuals' Personal Data is processed by Frontline, please contact the Legal and Compliance Manager

2.9.7 Policy 9 of this handbook records the various privacy statements used by Frontline.

2.10 Processing Relevant Data and Keeping it Accurate

2.10.1 Personal data collected shall be adequate, relevant and limited to what is necessary for the purpose for which it is processed. You must not collect and process more Personal Data than you need. For example, if you will never telephone someone at home, you do not need to record their home telephone number.

2.10.2 Personal Data (including any Special Category Data) you collect should be appropriate to, and sufficient for, the relevant purpose(s) you are collecting it for, but not excessive for that purpose(s).

2.10.3 In addition, you must take care to record and input Personal Data accurately. This is important. There can be serious risks for Frontline if Personal Data is incorrect. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date.

2.10.4 Where collecting Personal Data about an individual indirectly (e.g. from a published source), Frontline must still inform the individual that it holds the data and the purposes for which that data will be used.

2.11 Data Retention

2.11.1 Frontline cannot retain Personal Data longer than is reasonably necessary depending on the circumstances. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws). Other records must only be kept while in current use and for a reasonable period afterwards. In order to comply with law, you must comply with Frontline's Data Retention Policy.

2.11.2 As a general rule, when Personal Data is no longer needed by Frontline for the purposes for which it was collected, this Personal Data should be securely destroyed as soon as practicable.

2.12 Data Subjects Rights

2.12.1 Individuals have certain rights in relation to their Personal Data:

a. the right to access Personal Data held about themselves;
b. the right to prevent processing of Personal Data for direct marketing purposes;
c. the right to have Personal Data rectified if it is inaccurate;
d. the right to have their Personal Data erased (the 'right to be forgotten');
e. the right to restrict processing in certain circumstances;
f. the right to data portability in certain circumstances;
g. the right to compensation for any damage/distress suffered; and
h. the right to be informed of automated decision making about them and the right to object to such processing and to not be subject to automated decision making which produced legal effects concerning the individual.

2.12.2 If you should receive an enquiry about any of the above rights that you are unsure about, then you should seek advice from the Legal and Compliance Manager

2.12.3 Individuals are allowed to withdraw their consent to Frontline's use of their Personal Data at any time. However, Frontline will only be relying on consent to process Personal Data in very limited circumstances. Other lawful reasons for processing will be relied upon where possible. If an individual contacts you to withdraw consent, inform the Legal and Compliance Manager promptly to seek advice and stop using / processing that Personal Data in a way that is inconsistent with the withdrawal of that consent until you have received guidance from the Legal and Compliance Manager as to the necessary steps to be taken.

2.13 Subject Access Requests (SARs)

2.13.1 Under Articles 12 – 15 of the GDPR individuals can ask for copies of the Personal Data Frontline holds about them and other details about how Frontline uses their data. If Frontline receives such a request it must comply and send the information to the individual within 30 days. You must therefore immediately act on receiving such a request (whether it was requested verbally or in writing), by informing the Legal and

Compliance Manager who will ensure the correct process is followed. You must not deal with such requests in isolation.

2.13.2 A data subject can request from Frontline to:

a. Confirm whether or not their Personal Data is being processed, the purpose of the processing and categories of data processed,
b. Have access to that data (a copy is normally provided),

The data subject may also request:

c. The recipients or categories of recipient to whom the Personal Data have or will be disclosed, in particular recipients outside the EEA or international organisations,
d. Where possible the envisaged period for which the Personal Data will be stored, or the criteria used to determine that period,
e. The existence of the right to request rectification or erasure of Personal Data or restriction from processing of Personal Data concerning the data subject, or to object to such processing,
f. The right to lodge a complaint with the ICO,
g. Where the data was not collected from the Data subject, any available information as to the source,
h. Where Personal Data are transferred to outside the EEA or an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 of the GDPR relating to the transfer,
i. Information on the existence of any automated decision making, including profiling.

2.14 Data Loss or Security Breach Procedure

2.14.1 There are potentially significant repercussions for Frontline and the individuals affected arising from a data loss or security breach. Where this occurs or you suspect it may have occurred you must:

a. Immediately report the details to the Legal and Compliance Manager or Legal & Compliance Officer If unavailable then you must contact the COO or other senior manager, providing them with as much information as you have available;
b. It is important that this is done immediately as it may be possible to reduce the impact of the breach by remote deletion, removal or other means.
c. Follow their guidance on dealing with the security breach and keep them up to date with any further information about it that you become aware of;

d. Not approach any individual data subjects, suppliers, regulators or make any public announcements about the security breach incident without the prior agreement the COO.

Examples of data breaches or potential data breaches to report (this list is non-exhaustive):

a. Loss or theft of laptop, mobile phone, flash drive, cameras or other portable devices containing personal data;
b. Loss of paperwork in transit (post, courier or in person) containing personal data;
c. Personal information sent to the incorrect person(s) or organisation(s);
d. A virus or other malware attack;
e. You responded to an email which you later realised was not genuine;
f. An office burglary or imposter.

2.15 Disclosure of Data

2.15.1 Any disclosure of Personal Data is a form of processing. That means that the rules described above concerning fair and lawful use have to be satisfied. You must not disclose Personal Data to a Third Party outside Frontline unless that disclosure constitutes a lawful reason for processing and satisfies the information notice requirements as explained above. The Legal and Compliance Manager will be happy to discuss this with you. In particular, it is important to note that Personal Data and Special Category Data on programme participants must not be disclosed to parents/guardians without consent (and in the case of Special Category Data, written consent) to that disclosure being obtained from the participant in advance. This is the case regardless of whether the participant is over 18 or under 18. Such disclosures are likely to be a seen as a data breach. If there is an emergency or another urgent situation in which you feel it is necessary to disclose Personal Data (or Special Category Data) to a parent/guardian without consent being obtained, please liaise with the Legal and Compliance Manager to confirm that it is lawful to disclose in those circumstances.

2.15.2 There are some other exceptions to deal with disclosures such as those requested lawfully by police where the information is necessary to prevent or detect a crime. If you receive a request for information about an individual from the government, police or other similar bodies or from other investigators you should pass that request immediately to the L&C MANAGER to be dealt with. The application of the relevant

exceptions needs careful consideration. The burden is on Frontline to determine whether these apply.

2.15.3 Third parties and contractors should only have access to data as required by their job role. They are also bound by rules of confidentiality concerning access to Personal Data.

2.16 Transfer of Data to Countries outside the EEA

2.16.1 The GDPR contains special rules on whether Personal Data collected in the UK can be transferred to another country. Within the UK, there are restrictions on the transfer of Personal Data outside of the European Economic Area (such a transfer can happen, for example, where Personal Data is e-mailed outside the EEA or a database is hosted in the US). This is to make sure the Personal Data remains safe and the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

2.16.2 The fact that there will be transfers of Personal Data to other countries, especially to outside the EEA, should be clearly set out in the privacy notices described so that it is expected by the affected individuals.

2.16.3 Articles 44 – 50 GDPR covers the law regarding the transfer of data outside the EEA. For more information on overseas transfers please contact the L&C Manager.

2.17 Data Collection for Marketing Purposes

2.17.1 The collection of Personal Data for marketing purposes is largely governed by the Privacy and Electronic Communications Regulations.

2.17.2 A degree of care is need to identify what is defined as marketing. What staff might consider as legitimate information sharing can be seen as unwanted and unconsented marketing to the recipient. You should therefore, seek guidance from the L&C Manager.

2.17.3 Where Frontline intends to collect the Personal Data of individuals and use it for marketing purposes, this must be clearly stated in the privacy notice and the person

must give clear, informed and specific consent to show that they understand what they are being asked to consent to. This will normally be by a series of tick boxes allowing the person to select how they wish to be contacted. This is known as ‘opting in’. Boxes which require a person to tick if they do not want to be contacted, known as ‘opting out’ are no longer allowed and must not be used. Pre-ticked boxes which rely on an individual removing the tick if they do not consent to be contacted are also no longer acceptable.

2.17.4 Evidence of an individual’s consent to be contacted for marketing purposes should be retained and stored for as long as Frontline is sending them any marketing information. This may only be destroyed once the marketing relationship has finished.

2.17.5 Under Article 21 of the GDPR data subjects have the right to object to having their data processed for marketing purposes and so are entitled to ask to be deleted from any mailing lists.

Conflicts of interest and fraud policy

Section 1: Overview

1.1 Purpose

1.1.1 Frontline is committed to ensuring that it acts with integrity and has high standards of personal conduct. As such, it opposes and seeks to eliminate fraud by the way it conducts business, and seeks to ensure all trustees, staff and volunteers act appropriately when in receipt of gifts or where a conflict of interest arises.

1.1.2 Frontline aims to create a culture which deters fraudulent activity, encourages its prevention, promotes its detection and reporting, and ensures its response is appropriately documented.

1.1.3 This document establishes the expected conduct of all Frontline staff and trustees, in relation to deterring, reporting and detecting fraud and conflicts of interest. It sets out the policy and procedures for dealing with the risk of significant fraud or conflicts of interest.

1.1.4 This policy is also intended to help trustees discharge their legal duty to act only in the best independent interests of the charity. Although this legal duty does not extend to staff, the spirit of this duty is deemed to apply equally to staff.

1.1.5 This policy also describes the expected conduct of all Frontline staff and trustees, in relation to the offer and acceptance / receipt of gifts and hospitality.

1.1.6 Reference is made to other policies where appropriate.

1.2 Responsibilities

1.2.1 All staff and trustees are responsible for

1.2.1.1 declaring actual or potential conflicts or the reasonable perception of such conflicts as soon as reasonably and practicably possible;

1.2.1.2 the prevention and detection of any actual or potential fraud, and reporting such activity; and

1.2.1.3 avoiding any activity that could reasonably be anticipated to lead to an actual or perceived breach of this policy; and

1.2.1.4 Only accepting or offering, gifts and hospitality in accordance with this policy and reporting such activity in accordance with this policy.

Failure to comply with this policy may lead to disciplinary procedures in line with Frontline's disciplinary policy.

1.3 Definitions

1.3.1 For the purposes of this policy, the terms listed below will take on the meaning as defined here:

Board	The group responsible for the ultimate decision making on Frontline's activities and direction, consisting of trustees and employees as defined in Frontline's Articles of Association
Bribery and corruption	The offering or the acceptance of a reward, for performing an act, or for failing to perform an act, with the intention to induce or reward improper performance.
Conflict of interest	Any situation where a trustee's or employee's personal interests or loyalties, or the interests or loyalties which that

	trustee or employee owes to another charity or organisation, occurs at the same time as an interest or loyalty to Frontline.
Fraud	The intentional distortion of financial statements or other records by persons internal and/or external to the organisation, which is carried out to conceal the misappropriation of assets or otherwise for gain. Fraud is in fact intentional deceit and for this reason it cannot include negligence.
Fraudulent activity	Fraudulent activity is a general term covering fraud, theft, bribery and corruption, deliberate misuse or misappropriation of assets or anything that leads to a financial advantage to the perpetrator or others upon whose behalf they act, even if those others are in ignorance of the fraud.
Interest	Where a trustee or employee stands to benefit from their position at Frontline, due to a financial, non-financial, direct or indirect resulting gain.
Loyalty	Where a trustee's or employee's decision-making is influenced by another appointment, employment or association of that trustee or employee.
Staff	Any person employed or engaged under contract by Frontline.
Theft	The dishonest taking of property belonging to another person with the intention of depriving the owner permanently of its possession.
Trustees	Those persons engaged by Frontline to be independent members of the Board or sub-committee(s).

Section 2: Policy and procedures

2.1 Conflicts of interest

2.1.1 All conflicts of interest, whether actual, potential, or perceived, should be declared at the earliest possible opportunity.

2.1.2 All staff who have any interest in a matter which they are involved in as part of their duties for Frontline must declare the nature of their interest to their line manager and make the Legal & Compliance Manager aware. A decision will then be taken whether it is appropriate for that member of staff to continue working on that matter. In particular in accordance with Frontline's Procurement policy, members of the senior leadership team and all budget holders will be required to complete a declarations of interest form on an annual basis.

2.1.3 Requesting a declaration of interests from trustees will be a standing agenda item at all meetings of trustees. In addition, all trustees will be required to complete a conflict of interests form on an annual basis.

2.1.4 The interests of trustees should be listed in a register. A declaration of interests form is provided to keep the register up to date. This can be found attached as Annex 1 to this policy.

2.1.5 The declaration of interests register should be updated when any changes or new entries occur. The trustees are responsible for informing the Legal & Compliance Manager of any changes. This can be done by ad hoc completion of the declaration of interests form, or via the standing agenda item at Board meetings.

2.1.6 A declaration of interests form should be completed by any new trustee as part of their induction to Frontline.

2.1.7 A trustee who has any interest in a matter under discussion, which creates a real or perceived risk of bias, should declare the nature of the interest and withdraw from the meeting to allow the other trustees to decide whether their absence is necessary or appropriate.

2.1.7.1 Such a trustee may not vote on, or count towards quorum for, that particular matter.

2.1.8 A trustee who has any other interest which does not create a real risk of bias, but which might reasonably cause others to think it could influence their decision, should declare the nature of the interest, but may remain in the meeting, participate in the discussion and vote if they wish.

2.1.9 If a trustee fails to declare an interest that is known to the Chair or Legal &Compliance Manager, the Chair or Legal & Complaince Manager will declare that interest.

2.1.10 Where the trustees decide on a matter in which a trustee has an interest, all decisions will be made by majority vote. A quorum must be present for the discussion and decision.

2.1.10.1 The conflicted trustee will not count towards the quorum.

2.1.10.2 All decisions where there is a conflict of interest will be minuted accordingly to include:

- the nature, extent and value of the conflict;
- the discussion which took place; and
- the action taken to manage the conflict.

2.2 Gifts and Hospitality

The principle guiding this policy is that conduct in relation to gifts and hospitality should not create (or be perceived to create) a conflict of interest. In particular, conduct should not give the impression that an individual has been influenced by a benefit to show favour or disfavour to any person or organisation. In general, staff and trustees must not encourage or accept any gift, reward or benefit from any member of the public or organisation with whom they have been brought into contact through their official duties. The main exceptions to this rule are described in the remainder of section 2.2.

2.2.1 Acceptance of Hospitality

2.2.2 Hospitality can take a variety of forms, some of which staff and trustees may accept, some of which should be declined. Staff and trustees may be offered hospitality as a normal business practice in a way that is directly linked to their role. Examples of this kind of hospitality include the offer of refreshments at business meetings or the offer of lunch or dinner at the end of an official engagement. This kind of conventional hospitality may be accepted. Meeting refreshments and teas and coffees do not need to be disclosed.

2.2.3 Hospitality may be accepted where:

2.2.3.1 it is proportionate, reasonable and offered in good faith

2.2.3.2 recipients are not given any impression that they are under any obligation to confer any business advantage

2.2.3.3 there should be clear and transparent criteria

2.2.3.4 if over the value of £75, it must be approved by the LCM.

2.2.3.5 there should be clear records kept.

2.2.4 If any member of staff is in doubt about whether it is appropriate to accept any offer of hospitality, the advice of the LCM should be sought. Staff must never canvass or seek gifts or hospitality.

2.2.5 Acceptance of Gifts by staff

2.2.6 Staff may accept isolated and inexpensive (<£75) gifts from suppliers and clients. These will usually incorporate that supplier's or client's logo. Staff who are offered or receive a large number of inexpensive gifts, such as food and alcohol (hampers and bottles of champagne) should refuse them. Expensive gifts (with a value > £75) should not be accepted. Unacceptable gifts should be returned to donors.

2.2.7 Declaring the acceptance of a gift or hospitality

2.2.8 Trustees and staff must record being offered or accepting any gifts or hospitality by completing a Declaration of Gifts and Hospitality form. The Legal and Compliance team will retain completed forms to help protect Frontline and individual members of staff.

2.2.9 The only exception are the following items not requiring disclosure: Meeting refreshments; Calendars; Diaries; Key Rings; Umbrellas; Desk Organisers; Mugs; Stationery (including memory sticks); Coasters; Commemorative Books; Mousemats; Badges; Ties/Scarves; Baseball Caps; Pens; Courtesy Transport (as long as it relates to official travel).

2.2.10 Giving gifts and hospitality

2.2.11 Trustees and staff should refrain from offering any gifts or hospitality as a rule. There are limited circumstances in which offering gifts or hospitality may be acceptable such as to express thanks to staff in a partner organisation who have worked over and above what is required of them. Any such gifts of gratitude should be limited in value to £100.

2.2.12 Before any gift or hospitality is offered, a Request for Gifts and Hospitality form must be completed and approved by the Legal and Compliance Manager.

2.3 Fraud

2.3.1 The Director of Finance and Compliance has specific responsibility for overseeing the financial arrangements on behalf of the Frontline Board.

2.3.2 The main duties of the Director of Finance and Compliance are to provide the Board with on-going independent assurance that:

2.3.2.1 The financial responsibilities of the Board are being properly discharged;

2.3.2.2 The resources are being managed in an efficient, economical and effective manner;

2.3.2.3 Sound systems of financial control are being maintained; and

2.3.2.4 Financial considerations are fully considered in reaching decisions.

2.3.3 Frontline's Trustees' Report and Financial Statements must include an Independent Auditors' Report, providing a view as to whether the financial statements give a true and fair view and whether proper accounting records have been kept throughout the financial year. In addition, it will report on compliance with the accounting requirements of the relevant Companies Act and Statement of Recommended Practice.

2.3.4 Staff and trustees should report any conduct that is reasonably believed to give rise to actual or potential fraudulent activity. This should be reported to the Director of Finance and Compliance, or, where relating to the Director of Finance and Compliance, then the Chief Operating Officer.

2.3.5 If those individuals referenced in clause 2.2.4 are involved in the suspected or actual fraudulent activity, the Chief Executive Officer and Chair of Trustees should be informed.

2.3.6 Where the above process is not felt by the reporting person to be appropriate or satisfactory, the Whistleblowing policy should be referred to for further guidance on reporting incidents.

2.3.7 If there is concern or doubt about any aspect of a matter which involves actual or suspected fraud, whether a matter should be reported, or an ongoing investigation into suspected fraud, advice should be sought from the Director of Finance and Compliance.

2.3.8 The Director of Finance and Compliance will have primary responsibility for coordinating the initial response to allegations of fraud. Any investigation should be conducted in line with the Frontline Disciplinary policy. As part of the response the Head of People must be consulted with regarding potential employment issues. The Chair of FARC should be informed and kept updated regularly.

2.3.9 As soon as practicable after conclusion of the initial investigation, the investigation should be reported to the Chair of Trustees and Chief Executive Officer. This should also form an agenda item at the next Board meeting, and consideration of the investigation should be appropriately recorded.

2.3.10 Where fraudulent activity is deemed to have occurred, it should be considered whether it is appropriate to report the matter to any additional parties or authorities. These may include but are not limited to: police, Charity Commission and Department for Education.

Section 4: Annexes

4.1 Annex 1 – Declaration of interest form

Name: _____

Position: _____
I hereby declare that:

Please tick the relevant box and give details as required. Please note that if a member of your family or close relative has an interest that may result in a conflict of interest for yourself, this should also be declared.

☐ I have no financial or other personal interest, direct or indirect, in any company or organisation that has business dealings with Frontline or in any matter that raises or may raise a conflict of interest.

☐ I have a financial or other personal interest, direct or indirect, in a company or organisation that has business dealings with Frontline or in a matter that raises or may raise a conflict of interest. The details of this are given below.

Name or person/company with which you have an interest	**Nature of the interest**

I also acknowledge that I shall make another declaration to state any change in any matter contained in this declaration within one month after the change occurs.

Signed: _____

Date: _____

Frontline