Five Talents UK Ltd: Data Protection Policy

Five Talents U.K. Ltd. (“**Five Talents**”, “**we**”, “**us**”, “**our**”, **“the organisation”**) is committed to protecting personal privacy and this Privacy Notice sets out what personal data we collect, how we collect it, what we use it for and who we share it with. Five Talents is responsible for ensuring that it uses personal data in compliance with data protection laws, including (but not limited to) the UK General Data Protection Regulation and any other national, implementing or supplementing data protection legislation including but not limited to the Data Protection Act 2018.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers employed staff, trustees, and volunteers for Five Talents. By signing this policy, you confirm you have read and understood Five Talents’ Data Protection Policy and will act in accordance with it.

Introduction

By “personal data” we mean information which could identify a person such as name and contact details, donation history to Five Talents, and also information about a person’s connection with and interest in Five Talents (e.g. ‘introduced to us by John Smith’ or ‘met us at New Wine’ or ‘born in Kenya’ or ‘invited us to speak at his church’ or ‘went on trip to Uganda’). This is so that we can send supporters relevant updates and invitations to relevant events. Personal data does not include data where a person can no longer be identified from it such as anonymised aggregate data.

For the purposes of data protection legislation, Five Talents is considered the “data controller” of personal data processed in connection with this Privacy Notice. This means that we are responsible for deciding how we hold and use personal data. Our address is Five Talents, % Mary Sumner House, 24 Tufton Street, London SW1P 3RB. Should a person have any questions about this Privacy Notice, they can contact the CEO at the above address or on +4420 3808 7643.

This Data Protection Policy applies to personal data that we collect, use and otherwise process when people visit our website, attend an event, are introduced to us by an existing supporter or otherwise share personal data with us. We may provide supplemental privacy notices on specific occasions when we are collecting or processing personal data so that the person is fully aware of how and why we are using personal data. Those supplemental notices should be read together with this Data Protection Policy.

What information do we collect and what do we use it for?

The types of personal data we may collect, store and use are set out in the table below and in each case we have specified what we use it for and our ‘lawful basis’ for processing it. The law specifies certain ‘lawful bases’ under which we are allowed to use personal data. Most commonly, we will rely on one or more of the following lawful bases for processing personal data:

1. Where we need to perform the contract we have entered into with the subject;
2. Where we need to comply with a legal obligation;

3. Where it is necessary for our legitimate interests (or those of a third party) and the subject's interests and fundamental rights do not override those interests;
4. Where a person has consented to us doing so.

Description	**Why is the data held and what is it used for?**	**Basis for processing data (e.g. consent, Article 9(2)(d)**	**Who holds the data and who can access it?**	**What security controls are in place?**
Supporter name and email address in Mailchimp	Sharing Five Talents stories, reports, event invitations etc	Consent. Direct Marketing is defined by the ICO as any material which promotes the aims and objectives of the organisation and direct marketing by email always requires consent, under ePrivacy laws.	Only Five Talents employees who have signed Data Protection Policy can access data, using login/password	We have one log-in / password known only to FT employees. Mailchimp holds all data securely with high levels of security protection.
Donor/ Supporter contact info and donation history in Salesforce (our CRM).	So that FT can thank, report back to and engage with supporters appropriately, eg sending literature, event or meeting invitations and fundraising appeals. We will also add some 'leads 'and 'contacts' to Salesforce if they are introduced to us by an existing supporters, but we do not add them to bulk email campaigns via Mailchimp without consent. We would only send them personal messages. We will sometimes use LinkedIn or Google searches to identify points of connection or interest with potential donors or speakers.	Legitimate interest.[1] We believe Five Talents' supporters would reasonably expect us to keep records of their engagement with us, send them reports, thanks or new appeals. We also believe a person (including a Trust, Foundation or Corporate) would reasonably expect to be emailed personally (not Direct Marketing) after (for example) making a gift or attending an event. We do not believe this infringes their interests, rights or freedoms.	Only Five Talents employees who have signed Data Protection Policy can access data, using login/password. Occasionally consultants or volunteers might be given access to our CRM for a specific purpose but only after signing the Data Protection Policy and their account would be disabled after terminating the contract.	All Five Talents users have own accounts with unique password. Salesforce holds all data securely with high levels of security protection.

[1] See guidance at https://www.institute-of-fundraising.org.uk/library/gdpr-the-essentials-for-fundraising-organisations/ which shows charities can rely on 'legitimate interest' to send direct marketing

Brief notes of subject's relationship with Five Talents - which may include reference to their religion or ethnicity	So that FT can engage with supporters appropriately. For example, we would invite supporters born in Kenya to meet Kenyan partners, or supporters who are Christian to a faith-based event.	As above, but further through Article 9(2)(d)[2]	As above	As above
Gift Aid Declarations - held under donor's record on Salesforce.	For claiming Gift Aid	Legal requirement to keep as evidence for Gift Aid claim	As above	As above
Third party providers hold some donor details eg GoCardless, Zapier, Charity Checkout, CAF, Slack, Stripe, Squarespace, Stewardship, Xero, DocHub	These payment platforms are used to make it easy for donors to donate to Five Talents securely	Legitimate interest. We believes that Five Talents' donors would reasonably expect these details to be captured when they make a gift and it does not infringe their privacy rights	As above	We have log-in / passwords known only to FT employees. These platforms hold all data securely with high levels of security protection.
Employee details	We store copies of employee details to pay them, comply with HR law etc. Some details are handled by 3rd parties eg Payroll by Stewardship	Legal requirement	FT employees - and the third party provider (eg Stewardship for payroll) where relevant	Soft copies of some details are on the Drive. Hard copies in cupboard in locked office. Payroll information is only accessible by Senior staff using passwords
Hard copy archives	We keep audit records incl. eg letters with donor details and some original documents as archives	Legal requirement for audit records.	FT employees; held in a cupboard in office)	The office is kept locked, as is the building (which is alarmed).

[2] Article 9(2)(d) is a special processing basis which allows religious (amongst others) not-for-profit bodies to process data provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent. See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Google Suite - supporter / contact names and email addresses will be in our Gmail accounts and in some docs on the GDrive	We use Gmail for emailing supporters, partners, potential supporters etc. We store copies of thank you letters, grant application letters, reports etc in the Drive which will inevitably contain some personal contact details / data.	Legitimate interest. We believe people understand that we may email them personally when we have reason to believe they are interested in our work (NB not via DM campaigns but personally). We also believe people understand that correspondence, reports etc are often archived electronically.	As above	All Five Talents users have own accounts with unique password. Google holds all data securely with high levels of security protection.
Hard copies of thank you letters and other donor correspondence	These are usually kept only in the office short term and filed electronically if necessary, with hard copies being shredded. However, during COVID-19 when the office is shut, some post is being redirected to employees' homes and destroyed there	Legitimate interest - necessary in order to receive gifts, thank and bank.	A small number of employees within the team	The employees have signed the data protection policy and do not keep donor data at home longer than necessary for processing. It is then destroyed. This arrangement will cease once the office re-opens post-COVID.

Special categories of personal data

Certain categories of personal data, such as race, religion or health, are considered to be "special categories" of personal data as they are more sensitive types of data. We do not routinely collect, store or use special categories of personal data of our supporters. However, as noted in the table above, we may note in our CRM that a supporter attends a particular church (which may be considered to be data on a person's religion) or was born in a particular country (which may be considered to be data on a person's race). We record this data so that we can share the most relevant event invitations, updates etc with supporters. Of course a person can request us to delete any 'special category' data such as references to religion if they wish to do so; to do so, they should contact the CEO at the above address or on +4420 3808 7643.

We do collect data on the gender and ethnicity of our staff, trustees and applicants for staff posts or trusteeships. We may in future also monitor additional 'protected characteristics.' This is so that we can monitor our performance against Diversity and Inclusion benchmarks.

Please note that we may use a person's personal data without their knowledge or consent, in compliance with the above rules, if we are required by law to do so or if we reasonably believe that it is necessary to protect our rights and/or to comply with judicial or regulatory proceedings, a court order or other legal process.

What if a person does not provide the personal data we request?

If a person does not provide us with certain information when requested, we will not be able to keep them updated on our work, invite them to events, claim Gift Aid where appropriate etc.

Change of purpose

We will only use personal data for the purposes for which we collected it (as identified above in the *What we use this data for* column), unless we reasonably consider that we need to use it for another reason which is compatible with the original purpose. If we need to use personal data for an unrelated purpose, we will notify the person and we will explain the legal basis which allows us to do so.

How do we collect this information?

We typically collect personal data when a subject signs up to our mailing list (name, email address), makes a one-off or regular gift (name, contact details, bank details if they choose to give via direct debit or standing order), attend an event (name, email address) or are introduced to us by an existing supporter.

In addition, we may receive personal information about a person from third parties, such as Stewardship or CAF if a person chooses to make a donation using these platforms, or from Charity Checkout if a person donates via our own website.

With whom will we share a person's information?

We may share personal data with third parties where this is required by law, where it is necessary to perform our contract with a person, or where we have another legitimate interest in doing so.

We will need to share personal data with others including (for example):

- HMRC when we make gift aid claims
- Event venues which require a guest list, food allergy information etc
- A person's data may be held electronically by Salesforce (our donor database provider), Mailchimp (our email-list provider), Xero (our accounting software provider), Google (our email provider and also used for storing our electronic documents and archives), Charity Checkout (our online donation-processing provider), Slack (our instant messaging service), Zapier (software which allows our donation platforms and database to synchronise automatically, saving us money) and Metro bank (our bank),

All our third-party service providers are expected to take appropriate security measures to protect personal data in line with our policies.

We may share personal data with third parties, for example in the context of the possible sale or restructuring of the charity. We may also need to share personal data with a regulator or to otherwise comply with the law or a judicial process. We may disclose personal data if we are required by law to

do so or if we reasonably believe that disclosure is necessary to protect our rights and/or to comply with judicial or regulatory proceedings, a court order or other legal process.

If we become aware of a data breach, we will report it in accordance with the regulations.

International transfers of personal data

Personal data may be transferred to, and stored at, a destination outside the UK and/or the European Economic Area ("EEA"). It may also be processed by staff operating outside of the UK and/or the EEA who work for our affiliates or for one of our suppliers.

Where we transfer personal data to another country outside the UK and/or the EEA, we will ensure that it is protected and transferred in a manner consistent with legal requirements. In relation to data being transferred outside the UK and/or the EEA, for example, this may be done in one of the following ways:

- The country that we send the data to might be approved by the European Commission or the UK Government (as appropriate) as offering an adequate level of protection for personal data;
- The recipient might have signed up to a contract based on "model contractual clauses" approved by the European Commission or the UK Government (as appropriate), obliging them to protect the personal data; or
- In other circumstances the law may permit us to otherwise transfer personal data outside the UK and / or the EEA. In all cases, however, we will ensure that any transfer of personal data is compliant with data protection law.

If anybody requires further information about these protective measures they can request it from the CEO at the above address or on +4420 3808 7643.

How long will we retain personal information?

We will only retain personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal obligations.

If a person is on our mailing list (Mailchimp), we would keep their data on Mailchimp until they unsubscribe or otherwise request to be removed from the list. We may periodically 'clean' the mailing list of email addresses which 'bounce back' or subscribers who have not opened an email from us for a long time, in which case a person's data might be removed from the list as we would assume they were no longer interested in hearing from us. Of course they could re-subscribe at any time.

If a person is a donor to Five Talents or has been invited to one of our events, we may keep their data on Salesforce (our CRM) even if they stop giving, because we use it for statistical analysis which guides our strategic decisions (eg which events have been best attended, what trends can we see in regular giving, which part of the country do most of our supporters come from etc - this helps us work out where to invest our limited fundraising resources). However, if a person requests to be removed from the CRM, of course we would do so. We would also cease sending a person updates about our work if they requested / opted-out. If a person had not made a gift for several years, we may assume that they are no longer interested and cease sending them updates etc even if they have not opted out. By law we have to keep basic information about our donors for six years after they cease being donors for tax purposes, if we claim tax relief (Gift Aid) on the donor's donations. We also have to keep financial

records for six years and these may include some personal data, eg our bank statements may include a donor's name if they gave that as a reference when they set up a standing order to us.

A person's rights in relation to their personal information

It is important that the personal data we hold about a person is accurate and current. We ask our contacts to let us know if their personal data changes during their relationship with us.

A person has rights as an individual which they can exercise in relation to the information we hold about them under certain circumstances. These rights are to:

- Request **access** to their personal data (commonly known as a "data subject access request") and request certain information in relation to its processing;
- Request **rectification** of their personal data;
- Request the **erasure** of their personal data;
- Request the **restriction** of processing of their personal data;
- **Object** to the processing of their personal data;
- Request the **transfer** of their personal data to another party.

If a person wants to exercise one of these rights, they should contact us at our office (contact details above).

A person also has the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Fees

A person will not usually have to pay a fee to access their personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if their request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from a person

We may need to request specific information from the person to help us confirm their identity and ensure their right to access the information (or to exercise any of their other rights) can be met. This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where a person may have provided their consent to the collection, processing and transfer of their personal data for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. To withdraw their consent, they should contact us % Mary Sumner House (contact details above). Once we have received notification that a person has withdrawn their consent, we will no longer process their information for the purpose(s) they originally agreed to unless we now have an alternative legal basis for doing so .

Changes to this Data Protection Policy

We reserve the right to update this policy at any time. We will notify signatories when we make any substantial updates. We may also notify people in other ways from time to time about the processing of their personal data.

IT Security

As so much of the data Five Talents holds is held electronically, it is important to ensure that it is held securely. Five Talents staff and volunteers all use their own personal laptops / Macs for work and inevitably travel with them. Staff also access emails on their phones and this IT security policy applies to all devices used for work. All staff must[3]:

Malware / Firewalls

- Update your operating system and applications regularly. If a security update is released, install it as soon as is practically possible.
- Keep your computer firewall switched on. For Windows users, make sure you install anti-malware software (or use the built-in Windows Defender) which includes a firewall and keep it up to date. For Mac users, use the built-in firewall found under Security & Privacy and also install anti-malware software. Ensure your phone is also protected against malware too.
- Be very wary of links in emails or social media, think twice before clicking and only click if you are sure of the source. Don't open attachments from unknown sources.
- If you suffer a malware attack or any other 'data breach' eg losing your phone or laptop, inform CEO of Five Talents as soon as is practical.
- Don't use pirated software.
- Be very careful when using public wifi (hotels, cafes etc). If possible use a VPN connection. If using your phone as a hotspot, ensure you have a password and check others are not connected.

File Storage

- Minimise the use of hard copy materials; only print if necessary and where any personal information is printed, keep these materials securely and privately, and dispose of them securely after use eg in the shredder.
- Store work files in the Google Drive which is protected and backed up by Google
- Only share Google-documents with external users where necessary, using their specified email address rather than the 'public on the web' function.
- If you store any Five Talents files containing personal data on your hard drive, you must add disk encryption eg a BIOS password (required when booting your laptop). But as a rule, any Five Talents files containing personal data should NOT be stored on your hard drive.
- Delete personal data (eg CVs from applicants) from the Drive when no longer required and in line with data retention policy.
- Only download Five Talents data if absolutely necessary and delete immediately after use, especially if personal data is involved

[3]SOURCE: https://www.pensar.co.uk/hubfs/Free_business_IT_security_policy_template_v5.pdf?t=1525841781890 – updated with help from Trevor Smith Jan 2022

- Five Talents will run periodic audits of the Google drive to check who has access, and re-set any documents to private as required.

Passwords and accounts

- Don't use an administrator account on your computer for everyday use - use your own log in details for all applications. Only use an administrator password for administrator tasks.
- Set a password or use other security (eg, fingerprint / face recognition) to unlock your device whenever possible.
- Manually lock your device(s) whenever you step away from them in shared or public spaces. Set your computer and phone to lock automatically after 5 minutes maximum and require a password to unlock.
- Change default passwords and PINs on computers, phones and all network devices
- Don't share your password with other people or disclose it to anyone else
- On rare occasions where passwords do need to be shared due to limited numbers of accounts, these should be shared via LastPass and only to people with Five Talents email addresses you know should be allowed access. The list of shared passwords should be reviewed annually.
- Store passwords to all Five Talents accounts in LastPass, ensuring they are strong passwords - at least three of upper and lower case letters, numbers and symbols, at least 8 characters long. Change them regularly, and don't use the same passwords repeatedly or re-use previous passwords. Do not use obvious words (password, Five Talents), sequential numbers or letters (11111, abcde) or keyboard sequences (qwerty) in passwords. Avoid writing down PINs and passwords. If you do store them safely and away from computers or phones.
- Ensure LastPass, Salesforce, Xero and Gmail are set to require Two-Factor Authentication, and log out of each immediately you have finished using them.
- Do not set any applications (Gmail, Salesforce etc) to open automatically - ensure you key in the password every time.
- Don't disclose passwords and other confidential information unless you are sure you are on a legitimate website.
- When a member of staff leaves Five Talents, their access to LastPass should be suspended and the passwords to all of their Five Talents accounts should be changed (if the accounts need to remain open; otherwise the accounts should be deleted).
- When a new member of staff joins Five Talents, they will be given access to LastPass and then they will be enabled to set up logins and passwords (for the accounts they need to be able to access only, and with two factor authentication where required.
- Five Talents will conduct an annual review of LastPass to ensure that all passwords are only accessible by those who ought to have access.

Care of devices

- Take particular care of your computer and mobile devices when travelling.
- If any device belonging to Five Talents is stolen, change all passwords immediately, execute remote-wipe function (ensure this is set up on your phone where operating system permits) and inform the CEO of Five Talents.

Guidance for Trustees and Volunteers

- Trustees, Advocates and other Volunteers may be given access to certain documents held on the G-Drive, via their personal email address. These documents may sometimes contain sensitive information and personal data. They should not share these documents with anybody

outside of Five Talents, and delete all downloads immediately after use. They should also follow good practices with all personal devices, including installing anti-virus protection, always using strong passwords and two factor authentication where appropriate.

General

- This IT policy will be reviewed annually and all staff will be asked to confirm they are following it by signing it annually.
- One trustee on the Board will be the designated Cyber Security lead. At present this is Toyosi Ariyo.

By ticking this box, I confirm I have read and understood Five Talents' Data Protection Policy and will act in accordance with it.

Name:

Date:

Role: Staff / Trustee / Volunteer / Other (please specify)

INTERNAL: UPDATED / REVIEWED [DATE]	RESPONSIBLE	NEXT INTERNAL REVIEW	EXTERNAL: UPDATED / REVIEWED [DATE, BY]	NEXT EXTERNAL REVIEW
May 24 2023	CEO	May 2024	Simmons & Simmons Law Firm, September 2021	September 2024