INTRODUCTION

This Policy ("**Policy**") sets out the Data Protection Principles which **The Crossroads Project (the charity)** commits to comply with when processing personal data in the course of its business of providing charitable services.

The Charity has notified its data processing activities to the Information Commissioner's Office under registration number: **C1411310**. The Charity has taken the decision at Board of Trustees level not to appoint a Data Protection Officer. The Charities Data Protection contact is Tracey Armitage Trustee.

COMPLIANCE WITH THIS POLICY

The Charity will ensure the protection of personal data in accordance with this Policy by all Volunteers and Suppliers.

A breach of data protection laws by the Charity, or by any Volunteer or Supplier could result not only in monetary penalties awarded against the Charity but also negative publicity for the Charity as well as for the charitable sector generally.

THE DATA PROTECTION PRINCIPLES

The Charity shall comply with the following Data Protection Principles when processing personal data.

1. **Fairness and Transparency:** The Charity must process personal data fairly and provide individuals with information about how and why their personal data is processed.

The Charity must provide a privacy notice to each client, Volunteer and Supplier to inform them of:-

- the identity of the Charity as data controller;
- the purposes for which their personal data is processed;
- the legal basis for processing;
- any legitimate interests pursued by the Charity or a third party, if applicable;
- the recipients or categories of recipients of the personal data, if any;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent at any time, if applicable;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
- the existence of Automated Decisions, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

For example, such privacy notice should be included in each volunteer induction pack. The privacy notice can also be made available on the Charity website or in other appropriate and easily accessible forms. If the notice is published on the website, a conspicuous link to the

website or privacy notice should be included in the Charity email footer or other stationery to bring the notice to the data subjects' attention.

Where a client provides personal data of third party data subjects to the Charity, no notice will have to be provided to those third party data subjects by the Charity if such information must remain confidential subject to an obligation of professional secrecy. To the extent that no such obligation of professional secrecy applies, the Charity should place a contractual obligation on each volunteer and Supplier to ensure that such notice is provided to those third party data subjects on behalf of the Charity.

2. **Lawful Processing:** The Charity must only process personal data, including sensitive personal data, lawfully where it has a valid basis for the processing.

Generally, personal data must not be processed without a legal ground. In the context of the Charity, personal data is typically processed on the basis of:

- processing necessary for the performance of volunteer safety recording contact details and next of kin.
- processing necessary for the legitimate interests pursued by the Charity, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This ground may apply to the processing of the personal data of any third party data subjects whose personal data is provided by the client;
- a legal obligation to which the Charity is subject and where compliance with such obligation necessitates the processing of personal data by the Charity;
- data subject's consent, where such consent is procured from the client; and
- other legal grounds.

3. **Purpose Limitation:** The Charity must collect personal data only for a specific, explicit and legitimate purpose. Any subsequent processing should be compatible with that purpose, unless the Charity has obtained the individual's consent or the processing is otherwise permitted by law.

The Charity will typically process:

- the personal data of its clients as required for the purposes of providing its charitable services and the administration of its charitable relationships;
- the personal data of its Volunteers as required for the administration of the Trustees;
- the personal data of its Suppliers as required for the administration of its Supplier relationships; and
- the personal data of its clients, Volunteers and Suppliers as is necessary in order to comply with its legal obligations.

The Charity will generally not carry out any unsolicited electronic marketing, but to the extent it does, it will have to comply with the law.

4. **Data Minimisation:** The Charity must only process personal data that is adequate, relevant and limited to what is necessary for the purpose for which it was collected.

The Charity should place a contractual obligation on each client to ensure that only the minimum necessary personal data is provided in connection with the charitable services sought.

Where a client provides personal data that appears excessive in connection with the charitable services sought, the Charity will return such personal data to the client and request that an adequate record of personal data is provided.

5. **Data Accuracy:** The Charity must take reasonable steps to ensure personal data is accurate, complete, and kept up-to-date.

The Charity should place a contractual obligation on each client to ensure that any personal data provided in connection with the charitable services sought is accurate, complete and up to date.

The Charity will endeavour to keep an accurate record of personal data in relation to its clients and Volunteers.

6. Individual Rights: The Charity must allow individuals to exercise their rights in relation to their personal data, including their rights of access, erasure, rectification, portability and objection.

The Charity will ensure that all Individual Rights Requests are correctly identified and appropriately responded to, subject to any applicable exemptions.

7. **Storage Limitation:** The Charity must only keep personal data for as long as it is needed for the purpose for which it was collected or for a further permitted purpose.

The Charity will keep all records as long as required by applicable law or as may be necessary having regard to custom, practice or the nature of the documents concerned. For example, financial records shall be preserved for a minimum period of 6 years.

Save for personal data included in records which must kept for a prescribed period or preserved permanently in compliance with any legal obligations to which the Charity is subject, such as the obligation explained above, personal data shall be kept for no longer than necessary for the relevant purpose. For example, any Volunteer records should be kept for no longer than 6 years following the departure of a Volunteer, unless a longer retention is required under applicable law.

8. **Data Security:** The Charity must use appropriate security measures to protect personal data, including where third parties are processing personal data on our behalf.

The Charity will adopt the following security measures:-

Physical security measures

- ensure physical security of premises, e.g. locked office;
- keep documents in parts of the building not accessed by clients;
- reduce access privileges to only those needed;
- grant access to only such Volunteers and Trustees who need to have access in connection with their duties;
- dispose of documents using a confidential bin or through a cross cut shredder; and
- other appropriate physical security measures.

Organisational security measures

- provide training to Volunteers where appropriate; and
- other appropriate organisational security measures.

Technical security measures (These are currently in development)

- firewalls which are properly configured and using the latest software;
- regular patch management and OS updates;
- real-time protection anti-virus, anti-malware and anti-spyware software;
- user access control management by, for example, the UAC functionality in Windows, adopting principle of least privileges;
- unique passwords of sufficient complexity and regular (but not too frequent) expiry;
- encryption of all portable devices ensuring appropriate protection of the key;
- data backup; and
- other appropriate technical security measures.

The Charity will comply with the Policy "Appointing Suppliers" (in Appendix).

9. **Accountability:** The Charity must take steps to comply with, and be able to demonstrate compliance, with the Data Protection Principles.

The Charity will implement appropriate governance processes as set out in this Policy.

GOVERNANCE PROCESSES

In order to ensure that the Data Protection Principles are implemented the Charity shall adopt the following governance processes.

A. Documented Policies

In order to ensure compliance with Data Protection Principle 9 (Accountability), the Charity shall comply with this Policy and implement such other data protection policies and establish internal governance processes from time to time as may be required in order to operate the Charity in compliance with data protection laws.

B. Assurance

The Charity will ensure, by way of training or otherwise, that Volunteers carry out their tasks in a way that will ensure compliance with data protection laws. All Volunteers and each Supplier shall have access to this Policy and it shall have an obligation to comply with it.

Each Supplier will have to comply with data protection obligations in accordance with its service agreement including, where appropriate, a data processing agreement.

The Charity shall periodically review this Policy and other policies to ensure that they continue to comply with the relevant legal requirements.

C. Advice

Where necessary the Charity shall seek advice in order to ensure that its processes comply with data protection laws.

D. Third Parties

The Charity shall comply with the Policy "Appointing Suppliers" in relation to appointing any third party contractor or Supplier who will process personal data on behalf of the Charity.

E. Data Protection Impact Assessments

The Charity shall implement a process so that any processing which is likely to result in a high risk to the rights and freedoms of individuals is subject to a documented Data Protection Impact Assessment (**DPIA**), to assess the risks associated with the proposed processing and identify any safeguards which should be put in place to mitigate those risks. The Charity shall maintain a record of each DPIA.

F. Record-keeping

The Charity will implement a process to maintain an up-to-date documented record of its processing activities by way of adding relevant information to the client file or by other appropriate means. This record should include a general description of the following:-

Record keeping requirements	**Suggested record**
● The purpose of the processing.	● Typically, in relation to charitable transactions this will include processing to deliver client services;
● The categories of personal data and individuals to whom the data relates.	● a variety of mostly client and volunteer records.
● Where possible, the envisaged retention period for the personal data.	● records will be retained as long as required by applicable law or as may be necessary having regard to custom, practice or the nature of the documents concerned; and
● Where possible, a general description of the technical and organisational security measures in place.	● the measures in place as set out at paragraph 8 above.

Although it is envisaged that the Charity will act as data controller in the majority of cases, where it processes personal data on behalf of another person the Charity will make sure to maintain a record of its activities as a data processor and/or data controller. This record should include a general description of the following:

- The identity of the Charity and contact details.
- The categories of processing carried out on behalf of the third party.
- Where possible, a general description of the technical and organisational security measures in place.

G. Privacy By Design

When implementing a new processing activity, tool or functionality involved in the processing of personal data, the Charity will ensure, by contractual means or otherwise, that such activity, tool or functionality is designed and built in a way that allows the Charity to comply with the Data Protection Principles.

H. Complaint handling

The Charity shall implement a process to receive and handle enquiries and complaints from individuals and the supervisory authorities concerning the processing of personal data.

The Charity shall ensure that all enquiries and complaints are dealt with in a timely manner, in compliance with any applicable statutory deadlines.

APPENDIX: GLOSSARY

anonymous data	Data which does not relate to an identified or identifiable individual, or personal data which has been rendered permanently anonymous in such a way that the individual is no longer identifiable (even if the data was combined with other data held by the Charity).
Automated Decision	A decision which produces legal effects, or similarly significantly affects an individual, and which is based solely on the automated processing (including profiling) of their personal data.
Charity	Providing charitable support to the community
controller	A party which determines the purposes and means of the data processing.
data	Any information which is recorded electronically or, where recorded in a manual format (e.g. on paper), is organised by reference to an individual.
data subject	The individual to whom the personal data relates.
Individual Rights Request	A request from a data subject in respect of their personal data, e.g. to access, erase, or rectify their personal data, or object to its processing.
personal data	Any data relating to an identified or identifiable natural person. This can include (but is not limited to) names, addresses, email addresses, positions held, photographs, job applications, personnel files, occupational health records, opinions, and correspondence to and from an individual.
Personnel	All volunteers of the Charity at all levels, including, Trustees and volunteers, or third party suppliers.
processing	Any operation performed on personal data, such as collection, recording, storage, retrieval, use, combining it with other data, transmission, disclosure, or deletion.
processor	A party processing personal data on behalf of a controller, under the controller's instructions.
pseudonymised data	Personal data which can only be attributed to a specific individual by combining it with additional information (such as a key or other identifier), where the additional information is kept technically and logically separate from the pseudonymised data to avoid the individual being identified. Pseudonymised data remains personal data.
Sensitive or **special categories personal data**	Personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; biometric (e.g. fingerprints or facial recognition) or genetic information; or information about a person's health, sex life or sexual orientation, or relating to criminal convictions or offences (including allegations).
Supplier	Any external vendor, supplier, consultant or similar third party engaged to provide services to the Charity.

APPENDIX: POLICY – APPOINTING SUPPLIERS

INTRODUCTION

This Policy ("**Policy**") sets out steps that should be taken where a third party ("**Supplier**") is appointed to provide services in connection with, or to, the Charity (as defined below) and which may involve the Supplier processing personal data. This Policy will also apply if an existing Supplier is re-contracted on new terms or re-engaged on existing terms.

This Policy ("**Policy**") sets out the 9 Data Protection Principles which The Crossroads Project ("**Charity**") commits to comply with when processing personal data in the course of its business of providing charitable services.

The steps which must be followed are:

Step 1: Establish whether the Supplier is a Data Controller or a Data Processor

Step 2: Comply with data protection law requirements in the procurement process

Step 3: Check whether personal data will be transferred outside the European Economic Area (EEA)

Step 4: Complete the self-assessment checklist to ensure compliance with this Policy

This Policy does not apply if the Supplier's services do not involve the processing of personal data (for example where it is solely a contract for the purchase of goods, such as hardware).

STEP 1: IDENTIFY WHETHER THE SUPPLIER IS A DATA CONTROLLER OR A DATA PROCESSOR

Whenever it is proposed to appoint a Supplier to which this Policy applies, it is important to first identify whether the Supplier is a "Data Controller" or a "Data Processor".

- A **Data Controller** is a party that determines the purposes (that is, why the information is being processed) and means (that is, how the information is being processed) of processing. To identify this, one should ask: is the Supplier the controlling mind behind the proposed activity? Is the Supplier deciding what personal data will be collected and what it will be used for, or is it the Charity? Often it is the person who "owns" the personal data. Broadly speaking, whoever "calls the shots" in relation to the personal data is likely to be a Data Controller. In the majority of cases the Supplier will likely be a Data Processor of the Charity rather than a Data Controller. However, there may be situations where the Charity appoints a Supplier who will be a Data Controller, as is shown in the examples below.

- A **Data Processor** is a party that processes the personal data on behalf of the Data Controller. To identify this, one should ask: is the Supplier carrying out the processing *only* because it has been instructed to do so by the Charity? If so, the Supplier will usually be a Data Processor.

It is important to identify whether the Supplier is a Data Controller or Data Processor because:

- If a Supplier is a Data Controller it will be directly responsible for complying with EU data protection laws (for example ensuring that the processing of the personal data is fair and lawful, and enabling individuals to exercise their rights under data protection laws).

- If a Supplier is a Data Processor, it will still have some direct obligations under EU data protection laws. However, its primary obligations will be imposed under contract with the Data Controller, i.e. the Charity. The Charity will be legally responsible for all processing performed by its Data Processors, and so it is crucial that strict controls are placed on the Data Processor's actions.

EXAMPLES

SUPPLIER AS A DATA CONTROLLER

- A solicitor, accountant or similar professional appointed to provide services to the Charity.
- If the Charity employs Personnel, it may engage a pensions provider for Personnel.

SUPPLIER AS A DATA PROCESSOR

- Where the Supplier is a data storage provider.
- A translation service provider.
- A confidential waste disposal service provider.
- An IT contractor with access to confidential information of the Charity.
- If the Charity employs Personnel, it may engage a payroll services provider to streamline the payroll process.

SUPPLIER NOT ENGAGED IN "PROCESSING"

- As mentioned above, this Policy does not apply if the Supplier's services do not involve the processing of personal data as set out in the examples below.
- Purchase of goods such as hardware, office supplies and other goods.
- Couriers are not considered processors as long as they do not access personal data, i.e. they are handed a sealed envelope which they must not open. They are a mere conduit between the sender and recipient.

If the Supplier will be acting as a Data Controller:

As mentioned above, it is less likely that a Supplier will be acting as Data Controller and the majority of Suppliers will be Data Processors. However, if the Supplier is indeed a Data Controller:

- The contract with the Supplier should contain standard terms for Data Controllers set out in Appendix 2.
- Step 2 will not apply and Step 3, regarding data transfers, should be considered.

STEP 2: COMPLY WITH DATA PROTECTION LAW IN THE PROCUREMENT PROCESS.

Because the Charity will be responsible for the actions of its Data Processors, there are certain steps which must be taken to protect the Charity when appointing a Supplier who is a Data Processor.

In addition, when contracting with a Supplier who is a Data Processor, the Charity is under a legal obligation to ensure certain **mandatory provisions** concerning personal data are included in the contract with the Data Processor. These provisions are reflected in the standard Data Processing Agreement.

The following table outlines the practical steps which should be taken during the procurement process to ensure that data protection legal obligations are met.

STEP	WHAT DOES THIS MEAN IN PRACTICE?
Understand the nature of the data processing	Identify the types and amounts of personal data which the Supplier will have access to. The Supplier should only have access to the minimum amount of personal data they need to provide the services. If the Supplier will have access to payment card data, the agreement will also need to address compliance with Payment Card Industry Data Security Standard (PCI DSS).
Conduct due diligence on the Supplier	Choose a Supplier providing sufficient guarantees regarding information security and handling of personal data. It should be ensured the Supplier is able to provide appropriate security protection for the data, taking into account the nature of the personal data and any risks involved (for example, the consequences of a security breach).
Take additional precautions with special categories of personal data or card payment data.	Pay particular attention to security specifications for the contract if it involves processing special categories of personal data.
Ensure the written contract contains or incorporates the data protection clauses	The contract with the Supplier must include specific data protection language, as this is a **legal requirement** under EU data protection laws. If the contract is on the Supplier's standard terms, it will still need to be ensured that the necessary data protection language is included in the contract.
Note any data transfers outside of the EEA	If any personal data will be transferred outside the EEA (including where the personal data can be accessed remotely from outside the EEA), steps must be taken to ensure that the transfer is lawful. See Step 3 below.
Anonymise, pseudonymise or aggregate personal data if possible	These safeguards should be considered to help eliminate data protection risks whenever possible.

Limit access to the personal data	The Supplier should have appropriate access controls so that only those involved in the delivery of the services can access the personal data, and access rights are limited to that necessary for everyone's role.
Ensure the Supplier can assist with individual rights requests.	The data protection language in the contract must include an obligation on the Supplier to assist the Charity to enable individuals to exercise their individual rights. These include rights to access, rectify and erase their personal data, and object to it being used for a particular purpose. The Supplier must ensure that it can respect these rights (e.g. by rectifying or erasing personal data), when requested to by the Charity. The Supplier should also ensure that if it receives any requests in relation to personal data, these are promptly passed on to the Charity.
Check the Supplier's subcontractors	Essentially, it should be ensured that all data processing terms will be 'flowed down' to any subcontractor.
Provide notice of the data sharing unless this has been done already	Ensure that the arrangement with the Supplier is covered by the privacy notice given to Personnel or clients, as applicable. If the arrangement is not adequately covered by the existing notice, consider how to inform them prior to providing their personal data to the Supplier.
Charity monitors the Supplier's compliance throughout the appointment	Ensure there are reasonable steps in place which allow a Charity to monitor the Supplier's performance with its security and processing obligations. For example, the Charity may check the Supplier's website and look out for any relevant press releases from time to time and regularly (depending on level of engagement and associated risks) ask the Data Processor (e.g. pursuant to the Data Processing Agreement) for information such as a confirmation of the information security measures that the Data Processor has in place from time to time.
Establish what will happen to the personal data at the end of the relationship	If there is no longer a need to keep the personal data, because of the termination of the service relationship or because the law no longer requires it, it should be returned to the Charity. Make sure the contract terms provide for the return of the personal data to the Charity or purging upon request of the Charity.

STEP 3: CHECK IF PERSONAL DATA WILL BE TRANSFERRED OUTSIDE THE EEA

This Step 3 should be completed whether the Supplier will be acting as a Data Controller or a Data Processor.

In considering whether to appoint a Supplier, the following should be established:

- whether the Supplier is, itself, located outside the EEA; or
- whether the Supplier may *subsequently* transfer personal data outside the EEA (for example to the Supplier's subsidiaries or subcontractors).

A 'transfer' of personal data includes the following:

- allowing personal data **stored** in the EEA to be **accessed remotely** from a country outside the EEA (e.g. the US);
- relocating a database outside the EEA; or
- sending a data set (for example an Excel file) as an attachment to an email to a recipient outside the EEA.

Subject to the exceptions set out below, personal data should not be transferred from an EEA country to a non-EEA country unless there are means of providing appropriate safeguards for that personal data.

A small number of countries (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay) have been legally recognised to provide an adequate level of protection and personal data can therefore be transferred from the EEA to those countries. The list of "adequate" countries can be found on the Commission's website, here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

The US is also regarded as "adequate" if the US recipient (whether the Supplier or a subcontractor) is certified with the EU-US Privacy Shield, and their certification covers the type of personal data which will be transferred. If the Supplier wants to rely on Privacy Shield, the recipient's certification should be checked on the online list: https://www.privacyshield.gov/list. If the Supplier will be relying on Privacy Shield, ensure it is subject to an obligation to maintain its Privacy Shield status for the duration of the agreement (or ensure the relevant US recipient does), and is obliged to enter into an alternative transfer solution if Privacy Shield is no longer valid.

For countries outside the EEA and not listed above an alternative solution has to be adopted before personal data can be transferred. The most relevant to the Charity is likely to be requiring the non-EEA recipient to sign up to an approved set of international data transfer clauses, known as the 'EU Model Clauses'. Which version of the Clauses should be used depends on whether the Supplier is acting as a Controller or a Processor. The EU Model Clauses should not be amended by the parties. The Appendices will need to be completed prior to execution.

Summary of the contractual arrangements which must be in place:

Country in which personal data will be hosted in, or will be accessible from	**How to regulate processing by the Supplier**	**How to regulate transfers outside the EEA**
'Adequate' countries (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay)[1]	Use the standard Data Processing Agreement	N/A as the countries offer 'adequate protection'
Non-adequate countries (e.g. Australia, India, China, or US companies not registered with the Privacy Shield)	Use the standard Data Processing Agreement	Execute the applicable EU Model Clauses
US Companies who are certified with the EU-US Privacy Shield, and their certification covers the type of personal data being transferred	Use the standard Data Processing Agreement	Ensure the Supplier is obliged to remain certified with the Privacy Shield throughout the term of appointment, and to put in place an alternative arrangement if Privacy Shield is no longer valid

Exceptions In some circumstances transfers may be made without ensuring appropriate safeguards for the transferred personal data, as explained above. These exceptions will mostly concern transfers instructed by the client rather than transfers to a Supplier of the Charity.	
Explicit consent from data subject.	This will only apply where all personal data in the document to be transferred outside the EEA is the personal data of the client and no third party (unless such third party also consented). Consent has to be freely given, unambiguous, informed and confirmed by affirmative action or statement of the data subject. A record of the consent must be retained together with the assessment of possible risks of the transfer and the appropriate safeguards put in place in relation to the transfer.
Transfer is necessary for the performance of contract	This will apply only to contracts between the Charity and the data subject or another party on the data subject's request. In such cases, the Charity should obtain a warranty from the client to the effect that the client has obtained explicit and demonstrable consent from each other data subject whose personal data is included in the document which is subject to the transfer. This exception will also likely apply to transfers to foreign public authorities.
Transfer is necessary for important reasons of public interest recognised by law.	This will apply in very limited circumstances, such as in the case of the UK's substantial public interest in detecting and preventing crime.

[1] Japan and South Korea were excepted in 2018.

Information in public registers.	You can transfer overseas part of the personal data on a public register, as long as the person you transfer to complies with any restrictions on access to or use of the information in the register.
Transfer is necessary in connection with legal proceedings, legal advice or defending legal rights.	This may apply, for example, where documents are forwarded to a third party law firm in connection with legal proceedings or legal advice.

These are the main exceptions that are likely to apply. However, in some circumstances further exceptions may apply.

STEP 4: SELF-ASSESSMENT CHECKLIST FOR COMPLIANCE WITH THIS PROCEDURE

To ensure compliance with the requirements of this Policy, the self-assessment checklist in Appendix 1 should be completed.

Last updated August 2023

APPENDIX 1

SUPPLIER APPOINTMENT SELF-ASSESSMENT CHECKLIST

This checklist will help you determine whether this Policy has been complied with. If any of your answers is "No", further information from the Supplier or independent legal advice should be sought.

HAVE ALL ACTIONS BEEN TAKEN TO ENSURE THE COMPLIANCE OF THE NEW SUPPLIER APPOINTMENT?	**COMPLETED**
I have identified what types of personal data will be disclosed to the Supplier.	YES
I have identified whether the Supplier will act as a Data Controller or a Data Processor in this processing.	YES
I have ensured that our contract with the Supplier addresses data protection compliance in lieu of its role in the processing.	YES
I have ensured that the Supplier requires personal data only as much as needed to achieve the purpose for which the Supplier is appointed and not more.	NA
I have considered with the Supplier whether providing pseudonymised, anonymised or aggregated personal data is adequate for the processing.	NA
For the personal data which is sensitive personal data I have ensured that the Supplier will take additional security measures to protect this personal data.	YES
I have taken steps to ensure that the Supplier only allows those within the Supplier with a genuine 'need-to-know' to have access to the personal data.	YES
I have taken steps to ensure that the Supplier will keep logs or records regarding processing of the personal data, including who accessed the data, when, whether data was changed, deleted, etc.	NA
I have taken steps to ensure that the Supplier will store the personal data only as long as needed for the purpose and no longer.	YES
I have taken steps to ensure that all personal data will be purged, erased or returned at the end of the appointment.	YES
I understand what (if any) other parties will be involved in providing the services and have ensured that the data processing requirements will be flowed down to the subcontractor.	YES
The processing requires the personal data to be accessible outside the EEA. I have put a transfer solution in place (see Step 3).	NA
I have put in place an internal process to monitor the Supplier's compliance throughout the appointment.	YES
I have taken steps to ensure that the relevant individuals have been / will be informed that their personal data will be used for this appointment and disclosed to a Supplier.	YES

APPENDIX 2

STANDARD DATA PROTECTION TERMS: DATA CONTROLLERS

[*INSTRUCTIONS FOR USE: This clause is intended for inclusion in a services agreement where a Supplier will be acting as a Data Controller (i.e. it determines the purposes and means of the processing of the personal data from the Charity).*

"Data Protection Legislation"	shall mean all applicable laws relating to data protection and privacy including (without limitation) the EU Data Protection Directive (95/46/EC) as implemented in each jurisdiction, the EU General Data Protection Regulation (2016/679), the EU Privacy and Electronic Communications Directive 2002/58/EC as implemented in each jurisdiction, and any amending or replacement legislation from time to time;
"Customer personal data"	shall mean all personal data (as defined in the Data Protection Legislation) controlled by Customer which is processed by the Supplier in connection with the Services;

[Ensure the Services Agreement contains defined terms for "Agreement", "Services", "Supplier" (which must include all EU affiliates)]

1. DATA PROTECTION

1.1. In this clause [1], the terms "personal data", "process", "data controller" and "data processor" shall have the meanings set out in the Data Protection Legislation.

The Supplier acknowledges that it shall be acting as an independent data controller in respect of Customer personal data.

Without prejudice to clause [1.2], if circumstances arise whereby the Supplier is acting as a data processor on Customer's behalf the Supplier shall promptly, on request by Customer, execute written contractual commitments which meet the requirements of the Data Protection Legislation. Until such written commitments can be put in place, this clause [1] shall be interpreted to give the closest possible effect to the requirements of the Data Protection Legislation.

The Supplier shall comply with its obligations under the Data Protection Legislation in respect of Customer personal data. Without prejudice to the foregoing, the Supplier shall not process Customer personal data in a manner that will or is likely to result in Customer breaching its obligations under the Data Protection Legislation.

The Supplier shall only process Customer personal data for the purposes of performing its obligations under this Agreement and for which it was disclosed by Customer to the Supplier.

The Supplier shall not process Customer personal data outside the European Economic Area ("**EEA**") (including by way of remote access) without the prior written consent of Customer.