DATA PROTECTION POLICY

1. Introduction

1.1 Family Friends will uphold people's privacy rights and comply with legal and contractual obligations, while making effective use of personal data to support our charitable objectives. We will take a risk-based approach to data protection decision-making, keeping in mind the intent of data protection law and effective operational outcomes and adopting best recommended practice where there is ambiguity about minimal compliance requirements. We have assessed the criteria outlined in the General Data Protection Regulation (GDPR) and have concluded that we are not required to appoint a Data Protection Officer. Data protection responsibility and risk is owned by the board of Trustees with day to day tasks delegated to the Chief Executive. This Data Protection Policy has been approved by the board of Trustees.

1.2 Scope

This policy applies to all "processing" of "personal data" (such as names, addresses, contact details, date of birth) where Family Friends is the Data Controller.

1.3 Implementation

The Data Protection Policy comprises this policy document and the supporting policies, procedures and guidance to which it refers to throughout.

An index of supporting materials is outlined below:

- Record of Processing Activity (ROPA)
- Baseline of specific privacy information
- Privacy Impact Assessments

The requirements of this policy will be incorporated into Family Friends operational procedures and contractual arrangements.

1.4 Review

We will review this policy and the latest best practice every 24 months, or sooner in the event of legislative or organisational change. This process will also help in identifying areas of improvement.

1.5 Data Protection Fee – Registration

We pay the required data protection fee to the Information Commissioner's Office (ICO). Our Registration Number is Z8154709.

1.6 Legislation

The Privacy and Electronic Communications (EC Directive) Regulations 2003
General Data Protection Regulation (Regulation (EU) 2016/679)
Data Protection Act 2018

2. Accountability

2.1 Day to day responsibility for data protection is delegated to the Chief Executive who will act as the Data Protection Lead. Data protection risks will be included in the risk register.

2.2 The Record of Processing Activities (ROPA), rights request and breach logs will be reviewed by the Trustee Board on an annual basis.

2.3 Data breaches will be reported to the Chairman and to the board of Trustees without undue delay if notification to the Information Commissioner is required, or at the next Board meeting.

2.4 We will ensure volunteers and staff receive data protection training annually, to meet the training objectives included at Appendix 6. Any Trustee who also undertakes operational activities for Family Friends (such as assessing risk on whether or not Family Friends will work with a family or volunteer mentor/befriender or not) will also be required to complete training on Data Protection, Confidentiality and Information Security. The nature and extent of this training will be determined by the Trustee Lead for Data Protection and the Chief Executive on an annual basis.

2.5 All staff, volunteers, trustees, contractors and temporary workers, are required to understand and comply with data protection standards and procedures. These will be provided at induction and will be available as part of the Staff Handbook/in the electronic Policies & Procedures folder.

2.6 How we adhere to the data protection principles

2.6.1 Lawfulness, fairness and transparency

(a) We maintain a Record of Processing Activity (ROPA) which outlines our lawful basis for processing, and the special conditions for processing special category data, including health data.

(b) We recognise that children have the same rights over their data as adults. We recognise the additional protection that should be given to the processing of children's data, including determining the appropriate lawful basis for processing, the privacy information that should be provided to children, and the right to erasure.

(c) We recognise that the processing of service user's data for the purpose of providing the befriending and/or mentoring service poses a higher risk to the data privacy of those individuals, due to the special category data that is shared with us, and also due to the circumstances which the individuals may be in.

(d) The processing of service user's special category personal data, including health data, will be done on the basis of their consent, as the processing for the purpose of providing them with the befriending and/or mentoring service does not meet any of the other conditions for processing. The service user's consent will be obtained verbally at the initial meeting and will be recorded on the Salesforce system. We will also obtain the service user's consent to share their personal data when making referrals to partner organisations in order to secure specialist support.

(e) We will rely on the lawful basis of 'legitimate interest' when sending materials by post (including those which contain marketing messages). This is lawful and is in line with the guidance of the Information Commissioner's Office that legitimate interest can be relied on where we can show that is "proportionate, has a minimal privacy impact, and people would not be surprised or likely to object".

(f) While processing for the purposes of sending marketing messages direct to individuals **by email** would ordinarily be done on the basis of consent, in accordance with the Privacy and Electronic Communication Regulation (2003), Family Friends does not send such messages direct to individual service users or potential service users. We do send marketing messages to professional contacts including referrers, schools, counselling colleges and other voluntary organisations. The guidance from the Information Commissioner's Office is that sending direct marketing messages to business contacts by email or text (SMS) messages is permissible.

(g) We will always give our business and professional contacts the opportunity to stop receiving marketing messages.

(h) Whenever we are processing personal data on the basis of 'Legitimate Interest' we will carry out and make available on request our Legitimate Interest Assessment.

We are governed by UK-GDPR (United Kingdom General Data Protection Regulation) which covers the E-Privacy regulation and came into effect on 31 January 2020.

Section 3 of this Data Protection Policy details how we will fulfil our transparency obligations. We will check that our processing of personal data is 'fair' by reviewing feedback and complaints.

2.6.2 Purpose limitation

(a) Our ROPA outlines our charitable objectives, the purposes for which we process personal data to deliver those objectives, and a description of the processing activities we undertake for each.

(b) When a new purpose for processing personal data is identified, we will assess whether this is compatible with existing purposes, or whether we need to have a new lawful basis for processing.

(c) We will use the Protecture Data Protection Impact Assessment tool to determine whether a Data Protection Impact Assessment needs to be carried out for any new purposes for processing.

(d) Service user personal data is held separately to the supporter and professional contact data, so limiting the inadvertent inclusion of their data in the processing for marketing purposes.

2.6.3 Data minimisation

We will explain why we need the data when we are collecting it – whether on forms, face to face, online or by phone. This will help us to ensure that we are only gathering information that is needed for that specific purpose.

2.6.4 Accuracy

We use structured applications forms and interview questions (both face to face and over the phone) to ensure that the information we capture for the service users is consistent. We use the features of our Salesforce system to ensure that there is consistency and accuracy in data recording. We have clear procedures in place to respond to requests for individuals for rectification (see Appendix 1).

2.6.5 Storage limitation

(a) Our ROPA identifies a retention period for each purpose for processing. Our privacy information tells people how they can make a 'Right to Erasure' request and we have a procedure in place to deal with requests (see Appendix 1).

(b) When we no longer need information in a form that identifies individuals, we will anonymise the data.

(c) We have adopted the Institute of Records Management (IRMS) Toolkit and Retention Schedule to guide our management of business and personal data and in particular where there are statutory or recommended retention periods.

2.6.6 Integrity and confidentiality

Section 5 outlines our approach to data security.

3. Transparency

3.1 We provide privacy information to each of our categories of data subject:

- Service Users
- Staff
- Volunteers
- Trustees

3.2 We provide at least some privacy information at the point of collection of the data, including the purpose for the processing and who the data will be shared with. We ensure that the privacy information is:

- person-centred, not legalistic
- concise, transparent, intelligible and easily accessible
- written in clear and plain language.

We will regularly review and update privacy notices to reflect any changes in data processing activities.

4. Rights

4.1 We ensure that people are informed of their rights over their personal data by including this in our privacy information.

4.2 We have a procedure in place (Appendix 1) to identify and respond to the following rights requests:

- Subject Access
- Rectification
- Erasure
- Objection.

4.3 As soon as we receive an objection to direction marketing, we will stop sending out direct marketing to that individual and clearly mark their record. There are no exemptions or grounds to refuse this.

4.4 We currently do not have any processing of personal data which meets the criteria for Data Portability and Automated Decision Making.

4.5 We include identification of rights requests in training for staff.

4.6 We keep a log of rights requests.

5. Security and personal data breaches

5.1 The "nature, scope, context and purposes of processing" will be used to determine the "appropriate technical and organisational measures" that need to be taken in order to protect the personal data from unlawful or unauthorised processing and against accidental loss, destruction or damage.

5.3 We have a procedure in place (Appendix 2) to identify and respond to personal data breaches.

5.4 We include identification of breaches and how to respond to them in staff training.

5.5 The following policies describe how we protect information:

- Referral Form
- Policy 1 – Risk Management Report
- Policy 2 – Master Safeguarding Policy
- Policy 3 – Complaints Policy
- Policy 4 – Complaints Policy for Families
- Policy 5 – Grievance and Disciplinary Policy
- Policy 6 - Confidentiality Policy
- Policy 8 – Finance Policy and Procedures
- Policy 13 - Volunteer Policy
- Policy 14 – Volunteer Agreement
- Policy 16 – Volunteer Code of Conduct
- Policy 18 - Customer Care/User Involvement Statement
- Policy 19 – Family Agreement
- Policy 20 – Parent Consent Form

- Policy 24 – ICT Internet Safety and E Security Policy
- Policy 28 – Risk Assessment for Supporting More than Two Children
- Policy 31 - Referral Form
- Policy 33 – Photo Policy
- Policy 51 – Cyber Security Policy

5.6 Our contracts with third party suppliers including IT providers, accounting services, clinical supervisors, consultants and website managers outlines their security measures.

6. Our approach to working with suppliers and partners

6.1 When researching or negotiating with new suppliers, we will use the due diligence questions at Appendix 3 to ensure they comply with data protection standards.

6.2 We use Data Protection contract clauses (Appendix 4) for suppliers who are acting as Data Processors on our behalf.

6.3 When data is shared with or disclosed to other organisations, we will include this in our privacy information.

6.4 When data is shared with other organisations other than under contract we will use a data sharing agreement.

6.5 When we are joint data controllers with other organisations we will set out our respective responsibilities including for providing privacy information and handling rights requests.

7. Data Protection by Design

7.1 When we are introducing a new technology, a new service, or changing the way we do things, we will consider the potential impact on the data privacy of individuals and include data protection from the outset.

7.2 Before starting any high-risk processing activity, the decision as to whether a Data Protection Impact Assessment (DPIA) is required will be taken by the Chief Executive Officer and the board of Trustees based on the criteria described in the GDPR and the Article 29 Working Party Guidance on Data Protection Impact Assessment. The DPIA will be reviewed annually.

8. Our approach to transfers of personal data outside the EEA

8.1 We do not transfer data outside the EEA without a valid condition for processing and appropriate safeguards for the rights and freedoms of the data subjects.

8.2 Any processing which is done outside of European Economic Area will be documented in our ROPA.

8.3 We will ensure that any potential transfers outside of the EEA by data processors acting on our behalf is identified before we enter into a contract with them.

Appendices

Appendix 1: Procedure for Rights Requests
Appendix 2: Draft Information Incident Procedure
Appendix 3: Incident Reporting Form
Appendix 4: Data Protection Due Diligence: Supplier Checklist
Appendix 5: Data Protection Clauses
Appendix 6: Training Objectives

APPENDIX 1: Procedure for Data Rights Requests

1. Introduction

1.1 Rights Requests may come in any form – via email, face to face, by phone or in writing. We have to respond to requests without delay, and at the latest within one month. If requests are complex, we may be able to extend by up to a further two months, but we need to explain to the individual why we need the extra time. We expect that this will only be in exceptional circumstances and ordinarily we will work to the one month deadline.

1.2 Requests must be fulfilled **free of charge**. However, for subject access requests we can in exceptional circumstances charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive, or for further copies of the same information.

1.3 This procedure applies to the following rights requests:

- Rectification (Steps 1-5, 10)
- Objection (Steps 1-4, 6, 10)
- Subject Access (Steps 1-4, 7-8,10)
- Erasure (Steps 1-4, 9-10)

2. Responsibilities

2.1 All members of staff must be alert to individuals making rights requests. You may be in a position to check their identity (and they may be known to you), their authority and what type of request they are making (Steps 1-3). You should then pass the request to the Data Protection Lead, the Chief Executive without delay, with as much information as possible.

2.2 The Data Protection Lead will co-ordinate the response to the request, communicate with the individual and will keep the log of requests.

STEP 1: Check identity

Are you satisfied that the person is who they say they are?

- You can ask for sufficient information from the requester to enable you to confirm their identity. This is because you must only disclose personal information to the individual (or their representative – see 2. below). Do not discuss a request, or whether you do or do not hold personal information, until you are satisfied of the requester's identity. This is because even confirming that personal information is held could divulge information about someone.

STEP 2: Check authority

Are you satisfied that the person has the authority to make a request on behalf of someone else?

- This will be relevant when someone is (i) asking to see someone else's personal information, or (ii) is explicitly claiming to make a request on behalf of someone else. No individual has an automatic right to request access to someone else's personal information. However, someone can agree to a representative making a request for them (e.g. a parent for a child; a solicitor for their client; where there is power of attorney). You may need to check this authority.

STEP 3: Check the Request

What type of request is being made?

- People will not necessarily use the data protection jargon or the terms that are set out in the legislation. They may say they are making a 'freedom of information request' – when what they mean is subject access. They make ask for deletion, or removal, and what they want is for you to stop contacting them, or they may be making a request for erasure. If in doubt, clarify with them what they would like to happen.

- The rights which someone is able to exercise are linked to the lawful basis for processing. Check the ROPA to see the lawful basis and whether their request needs to be considered.

- Do you have enough information to locate what is being requested?

- You can ask for sufficient detail from the requester to enable you to locate the personal information they are seeking. However, you can't insist that they provide this. If you have personal information for a number of people with the same name, you could ask for further details from the requester (e.g. date of birth) to distinguish them from the other people.

- If the request is for 'all personal information' you could ask whether any specific information might satisfy the request, or that could be processed first.

Go to ***STEP 4***.

STEP 4 – Locate the personal information

Electronic system name	Result	If no personal information located – document

<ORGANISATION>Team consulted	Search undertaken	Result	If no personal information located – document

Data Processor consulted	Search undertaken	Result	If no personal information located – document

Hardcopy (paper) filing system name	Search undertaken	Result	If no personal information located – document

Go to **Step 5 for Rectification (correction), Step 6 for Objection, Step 7 for Subject Access and Step 9 for Erasure**.

STEP 5: Rectification

- The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

- If an individual has challenged the accuracy of their data and asked for you to rectify it, they also have a right to request you restrict processing while you consider their rectification request.

- If the personal data has been disclosed to third parties, we must inform them of the rectification, unless this is impossible or involves disproportionate effort. If the data subject asks, we must inform them about the recipients.

- Go to **Step 10**.

STEP 6: Right to Object

- Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority, direct marketing and processing for purposes of scientific/historical research and statistics.

- As soon as we receive an objection to direction marketing, we must make sure that we stop sending out direct marketing to that individual and clearly mark their record. There are no exemptions or grounds to refuse this.

- For other types of processing we must also stop, unless we can demonstrate compelling legitimate grounds for the processing, which override the interests of the individual, or the processing is for the establishment, exercise or defence of legal claims.

- If an individual exercises their right to object, they also have a right to request you restrict processing while you consider their objection request.

- Update the individual's record in Salesforce and/or other systems to ensure that the processing stops.

- Go to **Step 10**.

STEP 7: Review the Information

- Review the Information and identify any third party personal data that may be included. Can you disclose the personal information without disclosing information relating to, or identifying, anyone else?

- If it is not possible to separate the third party information from the personal information of the requester, can you consult the third party and ask for their consent? Note: You must be sure that the requester is happy for you to approach the third party – i.e. because in doing so, you will be informing the third party that the requester has made a request (which in itself could be something the requester wants to keep private).

- If the third party agrees that the personal information which involves them can be disclosed to the requester, keep a record of their decision. Even without consent, would it be 'reasonable in all the circumstances' to disclose the third party personal information to the requester? Is the third party owed or expecting confidentiality in relation to the personal information in question?

- There is an 'Assumption of reasonableness for health workers, social workers and education workers' in the Data Protection Act 2018. In practical terms this means that there is no necessity to remove the names of social workers from information being provided to service users who make a subject access request, when the social worker has been acting in their official capacity.

- Go to **Step 8**.

STEP 8: Review of possibly exempt personal information

- Are there any other reasons for wanting to withhold some or all of the personal information subject to the request? In general, the threshold for withholding personal information is high – common reasons are outlined below:

    - Information subject to legal professional privilege
    - Management forecasts: personal data processed for the purposes of management forecasting or management planning in relation to a business or other activity to the extent that the application of those provisions would be likely to prejudice the conduct of the business or activity concerned.
    - Negotiations: intentions of the controller in relation to any negotiations with the data subject to the extent that the application of those provisions would be likely to prejudice those negotiations.
    - Confidential references: Reference given (or to be given) in confidence for the purposes of the education, training or employment of the data subject, etc.
    - Journalistic, academic, artistic and literary purposes
    - Crime and taxation

- The full list of exemptions can be found in the Data Protection Act 2018

- Go to **Step 10**.

STEP 9: Erasure

- Individuals can ask for their personal data to be deleted, although the right to erasure (also known as the right to be forgotten) isn't an absolute right, and there are specific circumstances where you can refuse to meet their request.

- Particular attention should be paid to facilitating the right to erasure for children's data including where a child has given consent to the processing and they later request erasure. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent.

- You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to comply with a legal obligation
- the exercise or defence of legal claims
- for the performance of a task carried out in the public interest task or exercise of official authority
- for public health purposes in the public interest
- to exercise the right of freedom of expression and information
- archiving purposes in the public interest, scientific research, historical research or statistical purposes (if exercising the right to erasure would make it impossible or severely impair this processing).

- If the personal data has been disclosed to third parties, you must inform them of the erasure, unless this is impossible or involves disproportionate effort. If the data subject asks, you must inform them about the recipients. This includes online information - and Recital 66 of the GDPR specifically states that a data controller is "obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request".

- Even where it is not necessary or possible to comply fully with the request for erasure, it may be appropriate to erase some data – for example health data.

- Go to **Step 10**.

STEP 10: Respond to the Request

- Once completed, confirm to the individual that you have responded to their request and record the outcome in the Data Rights Log. If the request is refused, this must be explained to the individual, and we must also tell them how they can complain to the Information Commissioner's Office, or seek judicial remedy.

APPENDIX 2: Draft Information Incident Procedure

1. Introduction

1.1 This Procedure must be followed whenever there is an incident that **has or may** lead to accidental or unlawful loss, alteration, disclosure or access to organisational information.

1.2 A personal data breach has a specific meaning in legislation and therefore it is important to recognise when personal information is involved. This places specific responsibilities on the organisation in how to handle the incident.

1.3 An information security incident may involve personal data, but it may not. This Procedure is still applicable and will assist in dealing consistently with incidents and ensuring that lessons are learnt.

2. Responsibilities

2.1 All trustees, staff and contractors must:

- use this Procedure and the Incident Reporting Form to immediately report an incident which comes to their attention to the Data Protection Lead (DPL), namely the Chief Executive.
- consider if there is immediate action they can take to mitigate the damage (for example asking people who've received information in error to return or delete it).

2.2 The DPL will co-ordinate the response to the data breach:

- Gathering further information on the incident
- Assessing the risk to the rights and freedoms of individuals
- Notification to the relevant authorities
- Liaising with the relevant authorities
- Communication with individuals
- Documenting the Incident
- Reviewing the outcomes and learning lessons.

3. Gather Information

3.1 The DPL will receive the incident reports and if it's not immediately known, they must establish:

- What has happened and when
- What type of information has been lost and specifically whether this includes personal data
- If personal data is involved, the nature of that data and the number of people affected
- Any steps that have been or can be taken to reduce the damage.

4. Assess Risk

4.1 A breach of their personal information could pose a risk to individuals of physical, material, or non-material damage. This can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, or damage to reputation.

4.2 If the breach is **likely to result in a risk** to the rights and freedoms of individuals, then the Information Commissioner must be notified.

4.3 If the breach is **likely to result in a high risk** to their rights and freedoms, this needs to be communicated to the individuals **without undue delay**.

4.4 The DPL will work with the Board of Trustees to assess the risk and take the following factors into account:

- The type of breach
- The nature, sensitivity and volume of personal data
- Ease of identification of individuals
- Consequences for individuals
- Special characteristics of the individuals.

5. Notify

5.1 In the case of a personal data breach, the DPL must notify the Information Commissioner without undue delay, and within 72 hours of becoming aware of the breach.

5.2 If the notification is not made within 72 hours, the DPL must explain and document the reasons for the delay.

5.3 If a decision has been taken following the risk assessment exercise that notification to the Information Commissioner is not required then the DPL must record this.

5.4 The DPL should consider whether the police or other agencies such as the Charity Commission need to be notified.

5.5 Depending on the seriousness of the breach, trustees will be notified without undue delay, or at the next Trustee Board meeting.

6. Communicate

6.1 If the breach is **likely to result in a high risk** to their rights and freedoms, this needs to be communicated to the individuals **without undue delay**.

6.2 The DPL will co-ordinate communication with affected individuals and will ensure that this includes:

- a description of the nature of the breach
- a description of the likely consequences of the breach
- a description of the measures already taken or proposed to be taken
- any steps they can take to protect themselves from consequences
- a point of contact.

7. Document

The DPL will record in the Information incident log:

- A brief summary the incident
- Its cause(s) as far as have been determined
- What type of information was involved
- The consequences and mitigating and/or remedial action taken
- Whether notified to the authorities and whether there was any delay
- Whether communicated to individuals
- The reasoning behind decisions taken.

8. Review

8.1 Within four (4) weeks of the incident, the DPL will review outcomes and learning points, and will recommend updates to policies, procedures and training materials as appropriate.

8.2 The DPL will carry out a regular analysis of incident types which will form part of a report to the board of Trustees.

APPENDIX 3 Incident Reporting Form

Identifying an Incident:

- Destruction: where the data no longer exists, or no longer exists in a form that is of use
- Damage: where data has been altered, corrupted, or is no longer complete
- Loss: data may still exist, but the controller has lost control or access to it, or no longer has it in its possession
- Unauthorised or unlawful processing: may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data

Please complete as much of this form as you can then forward it to the Chief Executive at Family Friends without delay.

Name of the person reporting	
Contact details	
When (date and time) was the incident first noticed?	
What happened?	
What steps have been taken to stop or mitigate the damage?	
Was any business data affected?	
Was any personal data affected?	
How many people's personal data was affected?	
Was the information lost or unlawfully disclosed?	
Are there any risk to personal safety or financial loss for the people involved?	
When (date and time) was the Chief Executive Officer notified?	

APPENDIX 4: Data Protection Due Diligence: Supplier Checklist

Please complete the following questions, in order that we can understand your current approach to information security as required by Article 32(1) of the General Data Protection Regulation (implemented by the Data Protection Bill 2018).

The following are the minimum measures we will require assurance on:

1. Encryption and Data Minimisation
the pseudonymisation and encryption of personal data
2. Security and Access Control
the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
3. Backup and/or Business Continuity
the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
4. Monitoring, oversight and audit
a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Technical Measures Please provide us with the details of the **technical measures** you will employ when processing personal data on our behalf, including reference to the minimum measures set out above:
Organisational measures Please provide us with the details of the organisational measures you will employ when processing personal data on our behalf, including reference to the minimum measures set out above (for example, policies and procedures; staff training):

Location of Processing Where will our data be processed?
Please provide details of the countries, and locations within countries.
Please specify whether any data will be processed outside the EEA.
If the data will be processed in the United States, is the organisation committed to the EU-US Privacy Shield Framework?

Accreditations Please provide copies of any accreditations currently held
Please including details of any Statement of Applicability or details that confirms the nature and extent of the accreditation held (e.g. which office or service).

Record of Processing Activities (ROPA) Please provide details of the ROPA you currently maintain or confirm (i) you do not process any personal data on behalf of any other Data Controllers at present, or (ii) you have less than 250 staff and have decided not to maintain a ROPA.

Data Protection breaches Please provide details of the actual or suspected breaches you have had in the last year; whether any were reported to the ICO and/or the individuals affected, and what lessons were learnt as a result of the breach:

Data Protection contact Please provide the name and contact details for your Data Protection Officer or data protection lead (and EU Representative if applicable):

Name			
Position			
Company			
The answers provided are a fair and true representation of our technical and organisational arrangements			
Signed		Date	

APPENDIX 5: Data Protection Clauses

Definitions

Party	a Party to this Agreement
Agreement	this contract
Law	means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Contractor is bound to comply;
Contractor Personnel	means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any Sub-Contractor engaged in the performance of its obligations under this Agreement;
GDPR CLAUSE DEFINITIONS:	
Data Protection Legislation	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy;
Data Protection Impact Assessment	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer	take the meaning given in the GDPR;
Data Loss Event	any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach
Data Subject Access Request	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.
DPA 2018	Data Protection Act 2018
GDPR	the General Data Protection Regulation (Regulation (EU) 2016/679)
LED	Law Enforcement Directive (Directive (EU) 2016/680)
Protective Measures	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly

	assessing and evaluating the effectiveness of the such measures adopted by it
Sub-processor	any third Party appointed to process Personal Data on behalf of the Contractor related to this Agreement

Data Protection

1.1. The Parties acknowledge that for the purposes of the Data Protection Legislation, Family Friends is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is listed in Schedule [A] by Family Friends and may not be determined by the Contractor.

1.2. The Contractor shall notify Family Friends immediately if it considers that any of Family Friends' instructions infringe the Data Protection Legislation.

1.3. The Contractor shall provide all reasonable assistance to Family Friends in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of Family Friends, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4. The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule [A] unless the Contractor is required to do otherwise by Law. If it is so required, the Contractor shall promptly notify Family Friends before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by Family Friends as appropriate to protect against a Data Loss Event having taken account of the: (i) nature of the data to be protected; (ii) harm that might result from a Data Loss Event; (iii) state of technological development; and (iv) cost of implementing any measures;

(c) ensure that:

(i) the Contractor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule A);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they: (A) are aware of and comply with the Contractor's duties under this clause; (B) are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor; (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by Family Friends or as otherwise permitted by this Agreement; and (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU unless the prior written consent of Family Friends has been obtained and the following conditions are fulfilled:

(i) Family Friends or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by Family Friends;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Contractor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist Family Friends in meeting its obligations); and

(iv) the Contractor complies with any reasonable instructions notified to it in advance by Family Friends with respect to the processing of the Personal Data;

(e) at the written direction of Family Friends, delete or return Personal Data (and any copies of it) to Family Friends on termination of the Agreement unless the Contractor is required by Law to retain the Personal Data.

1.5. Subject to clause 1.6, the Contractor shall notify Family Friends immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or (f) becomes aware of a Data Loss Event.

1.6. The Contractor's obligation to notify under clause 1.5 shall include the provision of further information to Family Friends in phases, as details become available.

1.7 Taking into account the nature of the processing, the Contractor shall provide Family Friends with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by Family Friends) including by promptly providing:

(a) Family Friends with full details and copies of the complaint, communication or request;
(b) such assistance as is reasonably requested by Family Friends to enable Family Friends to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
(c) Family Friends, at its request, with any Personal Data it holds in relation to a Data Subject;
(d) assistance as requested by Family Friends following any Data Loss Event;
(e) assistance as requested by Family Friends with respect to any request from the Information Commissioner's Office, or any consultation by Family Friends with the Information Commissioner's Office.

1.8. The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:

(a) Family Friends determines that the processing is not occasional;
(b) Family Friends determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
(c) Family Friends determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9. The Contractor shall allow for audits of its Data Processing activity by Family Friends or Family Friends' designated auditor.

1.10. The Contractor shall designate a data protection officer if required by the Data Protection Legislation.

1.11. Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Contractor must:

(a) notify Family Friends in writing of the intended Sub-processor and processing;
(b) obtain the written consent of Family Friends;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause X such that they apply to the Sub-processor; and

(d) provide Family Friends with such information regarding the Sub-processor as Family Friends may reasonably require.

1.12. The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

1.13. Family Friends may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.14. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. Family Friends may on not less than 30 Working Days' notice to the Contractor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule A: Processing, Personal Data and Data Subjects

1. The Contractor shall comply with any further written instructions with respect to processing by Family Friends.
2. Any such further instructions shall be incorporated into this Schedule.

	Details to be specified by your Organisation
1. Subject matter	*A brief summary of the processing that the contractor is going to carry out on your behalf*
2. The purpose and nature of the processing	*Be as specific as possible about the purpose(s) for the processing and the activities that are going to be carried out* *Note: your organisation's ROPA should assist with this.*
3. Duration of the processing	
4. Categories of data subject	*For example: subscribers, donors, customers, staff.* *Note: your organisation's ROPA should assist with this.*
5. Categories of data	*For example: name, date of birth, address* *Note: your organisation's ROPA should assist with this.*
6. Return or deletion of the data	*Specify how long will the data be kept by the processor and how will it be returned or deleted*

Appendix No. 6 – Data Protection Policy
TRAINING OUTCOMES: STAFF, TRUSTEES & VOLUNTEERS

Key

A	Administrator
C	Chair
CE	Chief Executive
Op	Administrator & Chief Executive
S	Staff
TL	Trustee Lead
V	Volunteer Mentors/Befrienders
T	Trustees

Any Trustee who also undertakes operational activities for Family Friends (such as assessing risk on whether or not Family Friends will work with a family or volunteer mentor/befriender or not) will also be required to complete training on Data Protection, Confidentiality and Information Security. The nature and extend of this training will be determined by the Trustee Lead and the Chief Executive on an annual basis.

Privacy & Data Protection	Role	Information Security	Role	Confidentiality	Role	Training Outcomes Particular Roles	Role
I understand the background and purpose of privacy laws	**V, S & T**	I understand the importance of appropriate information security in the workplace	**V, S & T**	I know what the 'duty of confidentiality' is	**V, S & T**	I understand the purpose of PCI-DSS (Payment Card Industry - Data Security Standard) and how it applies to my work	**CE**
I am familiar with the Data Protection Principles and how to apply them in my role	**V, S & T**	I am aware of the organisation's Information Security policy and my responsibilities	**V, S & T**	I understand the principles of confidentiality	**V, S & T**	I know the DOs and DON'Ts of working with card payment data	**CE**

I know where policies and guidance on IG (Information Governance) are located and how to find help when I need it	**V, S & T**	I can recognise information security risks	**V, S & T**	I understand the differences between confidentiality and data protection	**V, S & T**	I know how to add new purposes and processing operations to the Records of Processing Activity	**Op**
I can assess whether or not information is 'personal data'	**V, S & T**	I know how to report an information security incident	**V, S & T**	I understand the importance of establishing the boundaries of confidentiality as early as possible	**V, S & T**	I am familiar with the process for requesting access to a colleague's email or home drive	**S**
I know how to recognise and report a data protection incident	**V, S & T**	I can identify and assess risks to the security of information assets I am responsible for	**V, S & T**	I am comfortable explaining the boundaries of confidentiality to customers and their families	**S**	I know how to respond to a request from a service user to see or obtain a copy of their record	**Op & TL**
I can recognise a subject access request, request for erasure of personal data or an objection to processing and know what action to take when I receive one	**S**	I can take appropriate steps to manage risks to the security of information assets I am responsible for	**V, S & T**	I know how to report a breach of confidentiality	**V, S & T**	I understand how the organisation's strategic goals are impacted by information risk	**CE, TL & T**
I understand how data protection applies to the personal data of employees (and volunteers)	**V & S**	I know the appropriate security precautions to take when accessing the organisation's ICT systems	**S**	I know where to go for advice on confidentiality and disclosures	**V, S & T**	I understand how the organisation manages information risk and am accountable for strategic information risk decisions	**CE, TL & T**
I understand how data protection applies to the personal data of our (customers / service users / beneficiaries / supports)	**S & T**	I understand the security compliance requirements that apply to my role and how to carry them out	**V, S & T**	I understand the need for employee privacy and confidentiality at work	**V, S & T**	I own the organisation's information risk policies	**CE, TL & T**

I know what a privacy notice is for and what it should contain	**S**	I know the Do's and Don'ts of working with high-risk data	**V, S & T**	I am aware of the situations where confidentiality may have to be over-ridden	**V, S & T**	I act as champion for information risk on the Board of Trustees	**TL**
I understand the rules for electronic marketing consent	**S**	I am familiar with the compliance standard for information security that apply to the organisation systems	**A**	I understand the need for balance between the privacy of the employee and the needs of the organisation	**S & T**	I oversee and am accountable for the organisation's data protection risk assessment and management processes	**CE & TL**
I know or can find information about the retention requirements for the personal data I work with	**V, S & T**	I understand key concepts and technologies in IT security	**A**			I lead and foster a culture that values, protects and uses personal data for the success of the organisation and the benefit of people associated with it	**CE & T**
I understand my data protection responsibilities	**V, S & T**	I can identify IT Security risks	**A**			I have a comprehensive understanding of data protection/privacy law	**CE & TL**
I know how to recognise and report a data protection breach	**V, S & T**					I maintain the organisation's Record of Processing Activity	**Op**
I know my data protection responsibilities as line manager	**S**					I monitor compliance with data protection requirements and report risks, issues, incidents and concerns to the Executive Board	**CE**
I can identify data protection risks	**Op & T**					I implement and lead the organisation's data protection risk assessment and management processes	**CE & TL**

I know that data protection risks must be considered early so they can be factored into plans and budgets	**Op & T**						
I recognise and understand data protection roles and relationships	**Op**						
I am aware of data protection considerations that are needed when work with external organisations involves personal data	**OP**						
I can assess the legal basis for processing personal data	**Op**						

Last updated January 2025