RIDGELINE TRUST CONFIDENTIALITY AND DATA PROTECTION POLICY
Reviewed and updated August 2021

1. The Aim of this policy:
For RT to be a charity which follows best practice, proportionate to its size. It is an aspect of respect for the clients, volunteers, staff, trustees, supporters and all whose *personal data* RT holds. (Italics mean that there is an explanation in the glossary at the end of this document.)
For RT to comply with the law, in particular with the new regulations which come into effect on 25 May 2018.

2. The legal basis for holding personal data
2.1. RT holds personal data of: clients, Members of the Charity, Trustees, staff, volunteers, supporters, and members of the Friends of Ridgeline scheme. That data may be *sensitive personal data*. Depending on what the information is, it may be particularly important that it is protected. Eg, a note that X has broken their leg is sensitive, but also obvious, whereas a note that X is receiving treatment for depression will not be obvious and may feel particularly private to X.
2.2. For staff, the legal basis for holding the personal data is that it is 'necessary for the performance of a contract with the staff member'.
2.3. For clients, the legal basis for holding the personal data is that it is 'necessary for the performance of a contract with the client' *and* that 'processing is necessary for the purposes of the provision of health or social care or treatment'.

Consent
2.4. For Trustees, Members of the Charity, volunteers, Friends and supporters, the legal basis is *consent*. RT will therefore have or obtain informed consent from those people. That consent has to be freely given, specific and easily withdrawn. RT will use an opt-in form.
2.5. RT will make it clear how a person can tell RT that they have changed their mind and withdraw their consent.
2.6. Consents will be reviewed and if necessary renewed in the event of a significant change of circumstances or changes in Ridgeline's activities.

2.7. Where a person's consent is not given, RT will record those facts – on a 'suppression list' – so that data is not shared or used when consent is needed but has not been given. Data will be checked against the suppression list before it is shared, for example, before a newsletter is sent out.

3. Using the data
3.1. RT will tell the person how it will be using the data (unless it is obvious).

3.2. RT will tell all individuals clearly and specifically who his or her data will be shared with. Clients will be told that data might be shared with people who look after them, but only if they need to know it. Data will not be routinely shared with volunteers; they will be given information that they need for safety or safeguarding.

Images
3.3. RT will not use a person's image without their explicit consent. Staff, members of the planning group and volunteers will be made aware of which clients and volunteers have/have not consented to use of their image.

4. Keeping personal data

4.1. Quality of records: Records, whether hard copy or electronic, must be factual, accurate and intelligible. RT will do its best to achieve this.

4.2. RT will not hold information that we do not need or is out of date. All personal data will be regularly reviewed as appropriate by the Trustees

5. When someone leaves: what we do about personal data

5.1. Someone may "leave" RT in various ways: a client stops coming; a member of staff leaves; a volunteer stops volunteering; a trustee resigns; a member/supporter does not want to continue as a member/supporter. This does not end RT's duty of confidentiality.

5.2. Personal data will be kept for six years from when a client or member of staff leaves, and one year in the case of everyone else. At the end of each financial year the Treasurer will delete from her records personal data of all clients, and members of staff who have left the organisation six or more years ago and volunteers who have left one or more years ago. A reminder to remove such personal data will be added to RT's annual programme for review of policies and procedures.

5.3. After that period, RT will keep "skeleton data", so that RT knows that it used to have that person's data. It may be useful if they return. For a client, RT will keep: their full name, their start and end dates, the funding source, and the date their personal data was shredded. For others, RT will keep: their full name, the start and end dates of their involvement with RT and their role, and the date their personal data was shredded.

5.4. Disposal: when personal data is disposed of, hard copies will be shredded and electronically held data deleted.

6. Who can have access to the personal data/ disclosing information

6.1. Anyone whose personal data RT holds can make a 'subject access request', ie a request to see what personal data RT holds on them. If a request is received on behalf of a client by someone who has responsibility for her/him, then the Chair or other designated person will assess whether it is appropriate to treat that request as if it had been made by the client.

6.2. The request may be received by email, or in writing, or orally, and will be responded to by RT within one month by the Chair or other designated person with responsibility for overseeing Data Protection .The first step will be to check the identity of the person making the request.

6.3. A record will be kept of all requests and when they were responded to. The person will be told what data is held and why, where it came from and who it is or will be shared with. If they want a copy they will be given a copy in a permanent form. If the request cannot be complied with for a lawful reason, that will be recorded. If anything needs to be redacted from the copy provided (eg because it is someone else's personal data) the reason for the redaction will be recorded. It may be sensible to devise a template for recording requests.

6.4. Personal data will be treated as confidential information, so it will be shared only on a need-to-know basis. This applies to sharing personal data within RT as well as outside RT. It will not be shared or used inappropriately with colleagues or outside work.

6.5. A family member, carer, social worker or other health professional might want access to personal data of a client. RT will seek the consent of the client to this happening unless it is necessary to share the information in an emergency situation. If it is not an emergency RT may share the information in the interests of public safety or the health and safety of another person. RT will take reasonable steps to ensure that the client knows and

understands what information is shared and with whom.
6.6. If it is necessary to give an outside body access to personal data then RT will do all it reasonably can to ensure that the third party respects the confidentiality of the data and complies with the law and the requirements of the ICO.
6.7. In a health emergency RT will share such information as is necessary for the individual's wellbeing with those who need to know, without the individual's consent if necessary.
6.8. If data is anonymised, ie it is not possible to identify individuals from the information, then it is not personal data, and the same legal requirements do not apply. RT will use anonymised data for research, funding or reporting purposes. RT will assess the risk of reidentification from anonymised data whenever it is using anonymised data.

7. Security against loss, damage and unauthorised access to personal data
7.1. Documents which contain personal data will all be password-protected.

7.2. Personal data will not be kept on memory sticks. A record of who has which RT memory stick will be kept.
7.3. RT will keep the RT premises secure.
7.4. Remote working:when working off-site, staff and Trustees will be aware of their work space and ensure no personal data are accessed by other people (e.g. family members)
7.5. If using a personal device to which others might have access, the member of staff or Trustee will take reasonable steps to ensure that other users of the equipment cannot access RT data.
7.6. Hard copies: documents at RT premises are in a locked drawer to which only people who might need to see the documents can access the key, and documents containing personal data of clients are to be kept there. They are not to be left out in circumstances where someone unauthorised could read them. Other documents which people print and keep at home, such as contact lists of trustees and staff, to be kept with a reasonable degree of security.
7.7. A record will be kept of when hard copies containing personal data which are normally kept at RT premises are removed from RT premises, who by and why, and when they are returned.

8. Ensuring compliance with the policy

8.1. A requirement to comply with this policy shall be a term of any employment or freelance contract, of any contract under which a person or company would have access to the personal data held by RT, and of all volunteer agreements, in terms appropriate for the role that the person has.
8.2. Training: RT will provide induction training for Horticultural Therapists and anyone in control of personal data, and refresher training as required

8.3. RT will put up reminders for staff and volunteers at RT premises.

8.4. Compliance with data protection law and with this policy will be built in to all new RT projects.
8.5. For group emails, the standard practice will be to use blind copies unless there is a good reason to let the others know who else is receiving it.

9. Personal data breaches
9.1. It is mandatory to report a breach to the Information Commissioner if it is likely to result in a risk to people's rights and freedoms. If that risk is *high*, then it is mandatory also to tell

the individual(s) concerned. A risk to someone's rights or freedoms could arise where the data includes:
date of birth, address, full name……risk of identity fraud
banking details……risk of financial loss
physical or mental health details……risk of embarrassment and exposure of confidential details
9.2. If a breach is suspected then the Chair of Trustees AND other designated person with responsibility for overseeing Data protection must be informed as soon as possible. That information must be shared with Trustees as soon as is practicable. Trustees will keep a record of all breaches and suspected breaches and what actions were taken.
9.3. When and how to report a breach: to the ICO. A breach has to be notified to the ICO as soon as possible (and within 72 hours of RT becoming aware of the breach at the latest) by the Chair of Trustees or other designated person with responsibility for overseeing Data protection.(ICO advises calling their helpline.)
9.4. If a breach has to be notified to the individual then it has to be done as soon as possible.
9.5. If the breach is sufficiently serious to warrant notification to the public, then RT will do so as soon as it can.
9.6. Breach of data protection as a risk appears on RT's risk register. The importance of a breach is high, but RT will aim to keep the likelihood of a breach low.

10. Who is responsible for this policy
10.1 The Chair Sara Uren is the designated data protection person and has overall responsibility for the issue of Data Protection at RT, assisted by another designated Trustee, Ros Richards

11. It is the responsibility of all staff, members of the Planning Group, volunteers and trustees to help each other give effect to this policy.

12. Glossary/notes
ICO = Information Commissioner's Office www.ico.gov.ukThe website contains useful guides, and there is a Helpline 0303 1231113
There is useful guidance on the website for the Social Care Institute for Excellence: https://www.scie.org.uk/care-act-2014/safeguarding-adults/sharing-information/
Personal data = information held on computer or in a filing system which relates to an identifiable, living individual, including any evaluation or expression of opinion about them. It can include an IP address and, in some circumstances, anonymised data.
Sensitive personal data = includes data which contains information about a person's racial or ethnic origin, religious beliefs, physical or mental health.
Consent: There is no "implied consent", silence does not mean consent, and it is not alright to have "opt-outs". Ie, RT cannot have a box on a form which a person has to tick if they don't want data held or used in a particular way.
A **personal data breach** is a 'breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.'

This policy is to be reviewed every year or earlier if required by changes in circumstances or Legislation

Policy approved by Trustees April 2018

Reviewed and approved by Trustees August 2021