RUSS Data Protection Policy

NOTE[1]

1. Policy Statement

Every day our business will receive, use and store personal information about our members, supporters, residents, stakeholders and colleagues. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

2. About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect or process.

This policy does not form part of any employee's contract of employment and may be amended at any time.

The Operations Director is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager or reported in line with the organisation's Whistleblowing Policy or Grievance Policy.

3. What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

4. Data Protection Principles

Anyone processing personal data, must ensure that data is:

a. Processed fairly, lawfully and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.
c. Adequate, relevant and limited to what is necessary for the intended purposes.
d. Accurate, and where necessary, kept up to date.
e. Kept in a form which permits identification for no longer than necessary for the intended purposes.

---

[1] Guidance from **www.uk.coop/gdprtoolkit**

f. Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
g. Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

5. Fair and Lawful Processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

6. Processing for Limited Purposes

In the course of our business, we may collect and process the personal data set out in the *Schedule 1*. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in the *Schedule 1* or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. Notifying Individuals

If we collect personal data directly from an individual, we will inform them about:

a. The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
b. Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
c. The types of third parties, if any, with which we will share or disclose that personal data.
d. The fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place.
e. How individuals can limit our use and disclosure of their personal data.
f. Information about the period that their information will be stored or the criteria used to determine that period.
g. Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
h. Their right to object to processing and their right to data portability.
i. Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
j. The right to lodge a complaint with the Information Commissioners Office.
k. Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
l. Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.
m. The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within 1 month.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data and our contact details are **info@theruss.org** and who the **Data Protection Compliance Manager** is.

8. Adequate, Relevant and Non-excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

a. Confirmation as to whether or not personal data concerning the individual is being processed.
b. Request access to any data held about them by a data controller (see also *Clause 15 Subject Access Requests*).
c. Request rectification, erasure or restriction on processing of their personal data.
d. Lodge a complaint with a supervisory authority.
e. Data portability.
f. Object to processing including for direct marketing.
g. Not be subject to automated decision making including profiling in certain circumstances.

12. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorised to use the data can access it.
b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the RUSS's DropBox, in password

controlled folders, instead of individual PCs.

Security procedures include:

a. **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
b. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
c. Data minimisation.
d. Pseudonymisation and encryption of data.
e. Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
f. Equipment. Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
g. Transferring Personal Data Outside of the EEA

We may transfer any personal data we hold to a country outside the European Economic Area ('EEA') or to an international organisation, provided that one of the following conditions applies:

a. The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
b. The data subject has given his consent.
c. The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
d. The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
e. The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14. Disclosure and Sharing of Personal Data

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

15. Subject Access Requests

Individuals must make a formal request for information we hold about them. Employees who receive a request should forward it to the Operations Director immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

a. We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
b. We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Where a request is made electronically, data will be provided electronically where possible.

Our employees will refer a request to their line manager [or the Data Protection Compliance Manager] for assistance in difficult situations.

16. Changes to this Policy, including monitoring and revew

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.

This privacy policy was adopted by the Board of Trustees and last updated on 28th February 2019.
This policy will next be reviewed by 28th February 2020.

This Privacy Policy will be available on our website at XXX.

THE SCHEDULE
DATA PROCESSING ACTIVITIES

Type of data	**Type of data subject**	**Type of processing**	**Purpose of processing**			**Type of recipient to whom personal data is transferred**	**Retention period**
Type of data collected	Type of Stakeholder	How we use the information	How we access the information	How we communicate with them	What is the purpose of this communication	Who do we share this information with	How long do we hold this information for
Personal or Organisational	**A: Members**	- Members are signed up to Slack forum - Members receive a Welcome email - Members receive a digital Share Certificate by email - Members are added to our MailChimp Newsletter database	Google drive Wordpress account Paper register (Name only) Paper shares file Paper membership forms file	Email Mailchimp Eventbrite Telephone	- Membership set-up - to validate their membership and receipt of payments - Regular Newsletter - to inform on RUSS activities and progress - Eventbrite for irregular events or fundraising - to inform and promote services and activities - Telephone for agreed actions or participating in events - to organise or respond to queries - Emails as needed - to organise or respond to queries	The Membership register is never shared with external parties.	Information is held until a mamber wishes to cancel their membership and withdraw their shares. Our Rules require 6 months notice of share withdrawal.
		- Members are uploaded as shareholders and/or donors to our Quick Books Online accounting system through our paypal account (Name only on QBO)	Paypal account				
Personal	**B: CGP Residents**	Additional:	Additional:	Additional:	Additional:		

Type of data	Type of data subject	Type of processing	Purpose of processing			Type of recipient to whom personal data is transferred	Retention period
	Church Grove Residents Group Financial assessments	In general terms, the data is reference material permitting management of the CGP residents group in terms of allocations of homes, assessment of applicants, reassessment of residents, contact with residents/applicants and the use of data to inform the development plan for the scheme.	Information for allocations is held on Dropbox in password protected area.			Information may be shared with Financial assessors such as Parity Trust or Ecology Building Society. But only confirmation of names as potential residents would be shared.	For the duration of residency. RUSS accounts may contain information which would need to be held for up to 7 years form final transactions.
	Church Grove Residents Diversity Survey					Individual information is not shared but some annonymised analysis may be shared in reports.	As above
Personal	**C: Self-build hub Volunteers**	Mailing people about hub meetings and volunteer opportunities, using to compile a skills audit for the build	Google drive & email	Email, mailchimp, trello - theres no data held on trello. People set-up their own logins to share project management information.	To let people know about meetings and organise volunteering	This information is not shared externally	Information will be held for the duration of the project plus 6 months

Type of data	Type of data subject	Type of processing	Purpose of processing			Type of recipient to whom personal data is transferred	Retention period
Personal or Organisational	**D: School attendees**	To communicate with prospective students and promote events To confirm bookings To take payments To share information among the group	Eventbrite Mailchimp Email Facebook Instagram	By Eventbrite By email By Facebook (sign-up)	Evenbrite - to sell tickets Email - to confirm and inform re event, answer queries Facebook - online forum	This information is not shared externally. However partner organisations may offer independant subscrptions ar a shared event.	Booking Information will be held until 6 months folowing the event it relates to. Personal data provided with consent will be kept on the school mailing list for as long as the School will offer educational opportunities.
	E: for Impact assessment?						