The Norwood Society Data Protection Policy

Aims of this Policy	The Norwood Society needs to keep certain information on its members, volunteers and those who attend its meetings, to carry out its day to day operations, to meet its objectives and to comply with legal obligations. The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation. This policy covers trustees, committee members, members, volunteers and any employees.
Definitions	In line with the Data Protection Act 1998 principles, The Norwood Society will ensure that personal data will: • Be obtained fairly and lawfully and shall not be processed unless certain conditions are met • Be obtained for a specific and lawful purpose • Be adequate, relevant but not excessive • Be accurate and kept up to date • Not be held longer than necessary • Be processed in accordance with the rights of data subjects • Be subject to appropriate security measures • Not to be transferred outside the European Economic Area (EEA) The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer systems. The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e. • **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data. • **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data. • **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained. • **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data. • **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.
Processing of Data	The Norwood Society processes the following personal information: Names and addresses, phone numbers, email addresses, subscription payment method, bank details, information required to claim gift aid and start date of membership.

	Personal information is kept in the following forms: Paper and computer based systems. Groups of people within the organisation who will process personal information are: Trustees and Executive Committee members.
Notification to the Information Commissioner	The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires. If there are any interim changes, these will be notified to the Information Commissioner within 28 days. The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is **Stephen Oxford**
Responsibilities	Under the Data Protection Guardianship Code, overall responsibility for personal data in a voluntary organisation rests with the governing body. In the case of The Norwood Society Executive Committee. The governing body delegates tasks to the Data Controller. The Data Controller is responsible for: • understanding and communicating obligations under the Act • identifying potential problem areas or risks • producing clear and effective procedures • notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes All Trustees and committee members who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles. Breach of this policy will result in the removal of Trustee status and/or the cessation of membership of committee members.
Policy Implementation	To meet our responsibilities Trustees and committee members will: • Ensure any personal data is collected in a fair and lawful way; • Explain why it is needed at the start; • Ensure that only the minimum amount of information needed is collected and used; • Ensure the information used is up to date and accurate; • Review the length of time information is held; • Ensure it is kept safely; • Ensure the rights people have in relation to their personal data can be exercised We will ensure that: • Everyone managing and handling personal information is trained to do so. • Anyone wanting to make enquiries about handling personal information, whether a member, volunteer, employee or service user, knows what to do; • Any disclosure of personal data will be in line with our procedures. • Queries about handling personal information will be dealt with swiftly.
Training	Training and awareness raising about the Data Protection Act and how it is followed in this organisation will take the following forms:

	• On induction: Trustees, committee members and members will be made aware of our policy. • General training/ awareness raising: Those gathering, storing and processing data will be trained in safe methods of doing so.
Gathering and checking information	Before personal information is collected, we will consider: whether the data is required for the running of the Society and how it will be stored and processed safely. We will inform people whose information is gathered about the following: • Why the information is being gathered. • What the information will be used for. • Who will have access to their information. We will take the following measures to ensure that personal information kept is accurate: • By regularly reviewing all data held • Deleting unnecessary data • Correcting inaccurate data Personal sensitive information will not be used apart from the exact purpose for which permission was given.
Retention periods	The Norwood Society will ensure that information is kept according to the following retention periods guidelines: Personal data of any form will only be held as long as membership is continued and will be deleted within six months of membership termination, except where required for taxation purposes.
Data Security	The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken: • Paper based data will be stored securely. • Computer based data will be stored on secure systems and not shared with anyone outside of the Society. • Any unauthorised disclosure of personal data to a third party by a member of the Executive committee may result in their dismissal from the Society. Data will be held securely using: • Lockable cupboards with restricted access to keys • Password protection on personal information files • Computer systems with restricted access • Secure methods of looking after personal data taken off site in any form • Secure backup systems. • Password protected attachments for sensitive personal information sent by email
Procedure in case of a breach	When a breach of data protection occurs, consideration will be given to reviewing practices. In addition The Norwood Society will consider whether the breach should be reported to the Information Commissioner.

Subject Access Requests	Anyone whose personal information we process has the right to know: • What information we hold and process on them • How to gain access to this information • How to keep it up to date • What we are doing to comply with the Act. They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong. Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to The Data Controller, The Norwood Society, secretary@norwoodsociety.co.uk We may make a charge of up to £10 on each occasion access is requested. The following information will be required before access is granted: Reason for requesting information We may also require proof of identity before access is granted. The following forms of ID will be required: • Photo ID, e.g. passport or driving licence and current utility bill or acceptable alternative Queries about handling personal information will be dealt with swiftly and politely. We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request and relevant fee.
Review	This policy will be reviewed annually to ensure it remains up to date and compliant with the law.
Declaration	I confirm I have read and understood The Norwood Society's Data Protection Policy and will act in accordance with it. I am connected with this organisation in my capacity as a ☐ Member of the Society ☐ Executive committee member ☐ Volunteer ☐ Trustee ☐ Other (Please state) _____ Signature:_____ Print name:_____ Date_____: Please return this form to the Secretary: