Voluntary Sector Studies Network
GDPR Data Protection Policy

The purpose of the GDPR is to ensure the "rights and freedoms" of living individuals, and to protect their personal data by ensuring that it is never processed without their knowledge and, when possible, their consent.

1. Scope

Voluntary Sector Studies Network (VSSN), its management and Steering Group, registered address at 289 Abbeydale Road Sheffield S7 1FJ, Sheffield, S2 2SE are committed to being fully compliant with all applicable UK and EU data protection legislation in respect of personal data. VSSN will safeguard the 'rights and freedoms' of persons whose information Voluntary Sector Studies Network collects through our members data base and associated communications, which are developed, implemented, maintained and periodically reviewed and amended by VSSN's Steering Group.

2. Objectives

VSSN's objectives for our members data base and associated communications are as follows:

1. To enable Voluntary Sector Studies Network to meet its personal data obligations in relation to how personal information is managed;
2. To support Voluntary Sector Studies Network's objectives;
3. To set appropriate systems and controls
4. To ensure that Voluntary Sector Studies Network is compliant with all applicable obligations, whether statutory, regulatory, contractual and/or professional; and
5. To safeguard personnel and stakeholder interests.

3. Good practice

Voluntary Sector Studies Network will ensure compliance with data protection legislation and good practice, by at all times:

1. Processing personal information only when to do so is absolutely necessary for organisational purposes;
2. Ensuring that the least possible amount of personal data is collected, and that personal data is never processed unduly;
3. Informing individuals of how their personal data is or will be used and by whom;
4. Processing only pertinent and adequate personal data;
5. Processing personal data in a lawful and fair manner;
6. Keeping a record of the various categories of personal data processed;
7. Ensuring that all personal data that is kept is accurate and up-to-date;

8. Retaining personal data no longer than required by statute or regulatory body, or for organisational purposes;
9. Giving individuals the right to access their personal data held by VSSN, as well as all other individual rights relating to their personal data;
10. Ensuring that all personal data is maintained securely;
11. Never transferring personal data outside of the EU
12. Identifying personnel that are responsible and accountable for our data processing.

4. Notification

As a not-for-profit Voluntary Sector Studies Network is exempt from the requirement to register with the Information Commissioner. However, it needs to comply with GDPR and VSSN has identified all of the personal data that it processes and recorded it in its Data Inventory Schedule.

This policy applies to all personnel of VSSN, including volunteers, Trustees, contractors and subcontractors. Breaches of the GDPR policy shall be dealt with by the Steering Group who will agree corrective actions which could include termination of contracts or expulsion from membership. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred to the relevant authorities.

All third parties working with or for Voluntary Sector Studies Network who have or may have access to personal data are required to read, understand and fully comply with this policy. All these third parties are required to enter into a Third Party data confidentiality agreement with VSSN. VSSN shall at all times have the right to audit any personal data accessed by third parties pursuant to the confidentiality agreement.

5. Responsibilities under the GDPR

Voluntary Sector Studies Network is both a Data Controller (it determines the purposes and ways personal data is processed) and a Data Processor (it processes personal data).Appointed personnel of VSSN with managerial or supervisory responsibilities are responsible for ensuring that good personal data handling practices are developed, reviewed and encouraged within VSSN, as per their individual role descriptions.

Data Controller

The role of Data Controller involves the management of personal data within VSSN as well as compliance with the requirements of the Data Protection Act and demonstration of good practice, and will be taken up by appropriately qualified and experienced members of VSSN's team.

VSSN's Steering Group acts as the Data Controller and, amongst other things, is accountable for the development and implementation of all data management systems and for day-to-

day compliance with this policy, both in terms of security and risk management. In addition, the Data Controller is directly responsible for ensuring that VSSN is GDPR compliant and that the VSSN Executive Officers are compliant in respect of data processing that occurs within their field of responsibility and/or oversight.

The Data Controller shall at all times be the first point of contact for any personnel of VSSN who require guidance in relation to any aspect of data protection compliance.

The Data Controller is also responsible for other procedures.

Members of VSSN are personally responsible for ensuring that all personal data they have provided and has been provided about them to VSSN is accurate and up-to-date.

Data Processor
It is not only the Data Controller who is responsible for data protection. All members and agents of Voluntary Sector Studies Network who process personal data are responsible for ensuring compliance with data protection laws.

Risk Assessment
It is vital that Voluntary Sector Studies Network is aware of all risks associated with personal data processing. VSSN will include data processing in its regular risk assessment process by carrying out an annual review of the Data Inventory Schedule. This review will assess whether all processes are being implemented, whether anything has changed and agreeing any actions needed. All planning meetings (events, projects) will include Data Protection issues as a standing agenda item. It is the role of the Data Controller to ensure that appropriate controls are in place to ensure that the risk level associated with personal data processing is kept to an acceptable level, as per the requirements of the GDPR.

VSSN is also required to carry out assessments of the personal data processing undertaken by other organisations on its behalf and to manage any identified risks, so as to mitigate the likelihood of potential non-compliance with this policy.

Where personal data processing is carried out by using new technologies, or when a high risk is identified in relation to the 'rights and freedoms' of natural persons, VSSN is required to engage in a risk assessment of the potential impact. If the outcome points to a high risk that VSSN's intended personal data processing could result in distress and/or may cause damage to data subjects, it is up to the Data Controller to decide whether VSSN ought to proceed and the matter should be escalated to the Steering Group via the chair. In turn, the Data Controller may escalate the matter to the regulatory authority if significant concerns have been identified.

6. Principles of data protection

The principles of personal data processing are as follows:

1. All personal data must be processed lawfully and fairly at all times.
2. Policies must also be transparent, meaning that Voluntary Sector Studies Network must ensure that its personal data processing policies, as well as any specific information provided to a data subject, are readily available, easily accessible and clear, drafted using clear and plain language.
3. The data subject must be provided with the following information:
    a. *Controller* - the identity and contact details of the Data Controller and any of its representatives;
    b. *Purpose* - the purpose or purposes and legal basis of processing;
    c. *Storage period* - the length of time for which the data shall be stored;
    d. *Rights* - confirmation of the existence of the following rights:
        i. Right to request access;
        ii. Right of rectification;
        iii. Right of erasure; and the
        iv. Right to raise an objection to the processing of the personal data;
    e. *Categories* - the categories of personal data;
    f. *Recipients* - the recipients and/or categories of recipients of personal data, if applicable;
    g. *Location* - if the controller intends to make a transfer of personal data to a third country and the levels of data protection provided for by the laws of that country, if applicable; and
    h. *Further information* - any further information required by the data subject in order to ensure that the processing is fair and lawful.
4. Personal data may only be collected for specified, explicit and legitimate reasons. When personal data is obtained for specific purposes, it must only be used in relation to that purpose.
5. Personal data must be adequate, relevant and restricted to only what is required for processing. In relation to this, the Data Controller shall at all times:
    a. Ensure that personal data which is superfluous and not necessarily required for the purpose(s) for which it is obtained, is not collected;
    b. Approve all data collection forms, whether in hard-copy or electronic format;
    c. Carry out an annual review of all methods of data collection, checking that they are still appropriate, relevant and not excessive; and

d. Securely delete or destroy any personal data that is collected in a manner that is excessive or unnecessary according to Voluntary Sector Studies Network's GDPR policies.

6. Personal data must be accurate and up-to-date:
   a. Data should not be kept unless it is reasonable to assume its accuracy and data that is kept for long periods of time must be examined and amended, if necessary;
   b. All personnel must receive training to ensure they fully understand the importance of collecting and maintaining accurate personal data;
   c. Individuals are personally responsible for ensuring that the personal data held by Voluntary Sector Studies Network is accurate and up-to-date. Voluntary Sector Studies Network will assume that information submitted by individuals via data collection forms is accurate at the date of submission;
   d. Any personnel of Voluntary Sector Studies Network are required to update the Office as soon as reasonably possible of any changes to their personal information, to ensure records are up-to-date at all times;
   e. The Data Controller must ensure that relevant and suitable additional steps are taken to ensure that personal data is accurate and up-to-date;
   f. The Data Controller shall, on an annual basis, carry out a review of all personal data controlled by VSSN, referring to the Data Inventory Register and ascertain whether any data is no longer required to be held, arranging for that data to be deleted or destroyed in a safe manner.
   g. The Data Controller shall also ensure that where inaccurate or out-of-date personal data has been passed on to third parties, that the third parties are duly informed and instructed not to use the incorrect or out-of-date information as a means for making decisions about the data subject involved. The Data Controller shall also provide an update to the third party, correcting any inaccuracies in the personal data.

7. The form in which the personal data is stored is such that the data subject can only be identified when it is necessary to do so for processing purposes. The following principles apply:
   a. Personal data that is kept beyond the processing date must be either encrypted or pseudonymised and kept to an absolute minimum, to ensure the protection of the data subject's identity should a data breach incident occur;
   b. Personal data must be retained according to the Retention Requirements Policy (below) and must be destroyed or deleted in a secure manner as soon as the retention date has passed; and
   c. Should any personal data be required to be retained beyond the retention period set out in the Records Retention Procedure, this may only be done with the express written approval of the Data Controller, which must be in line with data protection requirements.

8. The processing of personal data must always be carried out in a secure manner.

9. Personal data should not be processed in an unauthorised or unlawful manner, nor should it be accidentally lost or destroyed at any time and VSSN shall implement robust technical and organisational measures to ensure the safeguarding of personal data.

7. Security controls

Security controls are necessary to ensure that risks to personal data identified by VSSN are appropriately mitigated to reduce the potential for damage or distress to data subjects whose personal data is being processed. Security controls are subject to regular audit and review. Personal data shall not be transferred to a country outside of the EU.

8. Accountability

According to the GDPR accountability principle, the data controller is responsible both for ensuring overall compliance with the GDPR and for demonstrating that each of its processes is compliant with the GDPR requirements. To this extent data controllers are required to:

- Maintain all relevant documentation regarding its processes and operations;
- Implement proportionate security measures;
- Carry out Data Processing Impact Assessments (DPIAs which are carried out and recorded in the Data Inventory Schedule);
- Comply with prior notification requirements;
- Seek the approval of relevant regulatory bodies; and
- Appoint a Data Protection Officer where required. The level and scale of VSSN's activities currently do not require the appointment of a DPO.

9. The rights of data subjects

Data subjects enjoy the following rights in relation to personal data that is processed and recorded:

1. The right to make access requests in respect of personal data that is held and disclosed;
2. The right to refuse personal data processing, when to do so is likely to result in damage or distress;
3. The right to refuse personal data processing, when it is for direct marketing purposes;
4. The right to be informed about the functioning of any decision-making processes that are automated which are likely to have a significant effect on the data subject;
5. The right not to solely be subject to any automated decision-making process;
6. The right to claim damages should they suffer any loss as a result of a breach of the provisions of the GDPR;

7. The right to take appropriate action in respect of the following: the rectification, blocking and erasure of personal data, as well as the destruction of any inaccurate personal data;
8. The right to request that the Information Commissioner's Office carry out an assessment as to whether any of the provisions of the GDPR have been breached;
9. The right to be provided with personal data in a format that is structured, commonly used and machine-readable;
10. The right to request that his or her personal data is sent to another data controller; and
11. The right to refuse automated profiling without prior approval.

10. Data access requests

It is the right of all data subjects to ask VSSN the following:

1. What personal data VSSN is processing about that person, if any;
2. To be provided with a description of the personal data processed by VSSN about that person;
3. The purpose or purposes for which the personal data is being processed;
4. Confirmation of who will have access to the personal data; and
5. To be provided with a copy of the personal data, as well as a confirmation of where VSSN acquired that personal data.

VSSN will check that the request received is from the data subject before releasing the data requested.

VSSN has one month from the date of receipt of a Data Subject Access Request to provide to the data subject the personal data requested. Failure to provide the requested information within the one-month window is a direct breach of the GDPR. No extension shall be allowed under any circumstances.

Personal data exemption categories

The following data exemption categories apply, meaning that VSSN does not have to provide personal data covered below:

- The prevention and detection of crime;
- Negotiations with the data subject request maker;
- Management forecasts;
- Confidential references provided *by* VSSN however not references provided *to* VSSN;
- Data covered by legal professional privilege;
- Data used for research, statistical or historical reasons.

11. Complaints

All complaints about VSSN's processing of personal data may be lodged by a data subject providing details of the complaint directly with the Data Controller. The data subject must be provided with a Fair Processing Policy at this stage.

All complaints in relation to how a complaint has been handled and any appeals following the submission of a complaint shall be dealt with by the VSSN Chair and the data subject is required to submit a further complaint.

12. Consent

Consent to the processing of personal data by the data subject must be:

- Freely given and should never be given under duress, when the data subject is in an unfit state of mind or provided on the basis of misleading or false information;
- Explicit;
- Specific;
- A clear and unambiguous indication of the wishes of the data subject;
- Informed;
- Provided either in a statement or by unambiguous affirmative action;
- Demonstrated by active communication between the data controller and the data subject and never inferred or implied by omission or a lack of response to communication;
- In relation to sensitive data, consent may only be provided in writing, unless there is an alternative legitimate basis for the processing of personal data.

Personnel

Usually, Voluntary Sector Studies Network will obtain consent to process personal and sensitive data when a new contractor signs a contract or during induction programmes. Data subjects have the right to withdraw consent at any time. However certain data necessary for the performance of a contract needs to be kept by VSSN until it is no longer required to perform the contract or to comply with statutory regulations e.g. HMRC retention periods.

Other data subjects – Customers, supporters or members

If using Consent as a condition to process data Voluntary Sector Studies Network will obtain Consent in accordance with the procedures outlined in the policy framework. Consent is considered to be a positive action on behalf of the data subject having read a clear, transparent and unambiguous privacy notice. It does not necessarily have to be a box that is ticked, it could be the completion of a form, or the supply of contact information. We understand that according to Privacy and Electronic Communications Regulations (PECR) consent does not have to be explicit. We will use our judgement to decide how to obtain consent in different circumstances. For example, where a data subject has chosen to sign up to membership, provided their data and paid a membership fee it is reasonable to assume

consent to process their personal data in order to deliver membership services to them. However, we will always uphold the rights and freedoms of data subjects by always making it as easy to Opt-out as it was to Opt-in.

We mostly use Consent when promoting the aims and objectives of VSSN. We reserve the right to use it wherever we believe a data subject has indicated their wishes and where we have collected the data for that particular purpose. We only use data for the purpose for which it was collected.

13. Data security

All personnel of VSSN are personally responsible for keeping secure any personal data held by VSSN for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless VSSN has provided express authorisation and has entered into a confidentiality agreement with the third party.

Accessing and storing personal data

Access to personal data shall only be granted to those who need it and only according to the principles of this Policy.

All personal data must be stored:

- In a locked room, the access to which is controlled; and/or
- In a locked cabinet, drawer or locker; and/or
- If in electronic format and stored on a computer, encrypted and password protected and/or
- If in electronic format and stored on removable media, encrypted as per Disposal of Removable Storage Media
- If hosted online in electronic format, accessed through password protected log-in's for authorised personnel only and hosted by Cloud suppliers who VSSN has checked meet the required data security standards – currently we require Cloud suppliers to be ISO 27018 certified.

Before being granted access to any organisational data, all personnel of VSSN must understand and have a copy of this Policy.

Computer screens and terminals must not be visible to anyone other than personnel of VSSN with the requisite authorisation.

No manual records may be accessed by unauthorised personnel of VSSN and may not be removed from the business premises in the absence of explicit written authorisation. Manual records must be removed from secured archiving when access is no longer needed on a day-to-day basis.

All deletion of personal data must be carried out in accordance with VSSN's Retention Requirements as identified in the Data Inventory Schedule. Manual records which have passed their retention date must be shredded and disposed of as 'confidential waste' and any removable or portable computer media such as hard drives as USB sticks must be securely wiped or destroyed prior to disposal.

Personal data that is processed 'off-site' must be processed by authorised VSSN personnel, due to the increased risk of its loss, damage or theft.

14. Disclosure of data

Voluntary Sector Studies Network must take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the Police.

Disclosure is permitted by the GDPR without the consent of the data subject under certain circumstances, namely:

- In the interests of safeguarding national security;
- In the interests of crime prevention and detection which includes the apprehension and prosecution of offenders;
- In the interests of assessing or collecting a tax duty;
- In the interests of discharging various regulatory functions, including health and safety;
- In the interests of preventing serious harm occurring to a third party; and
- In the interests of protecting the vital interests of the data subject i.e. only in a life and death situation.

Requests from third parties for data should be referred to the Data Controller. The Data Controller is responsible for handling all requests for the provision of data and authorisation by the Data Controller shall only be granted with support of appropriate documentation.

15. Data retention and disposal

Voluntary Sector Studies Network must not retain personal data for longer than is necessary and once a contractor is no longer working for VSSN, it may no longer be necessary for VSSN to retain all of the personal data held in relation to that individual. Some data will be kept longer than others, in line with VSSN's data retention and disposal procedures detailed in VSSN's Data Inventory Schedule.

Personal data must be disposed of securely to ensure that the 'rights and freedoms' of data subjects is protected at all times.

Membership records retention requirements are:
VSSN will hold members data in the database and in the members directory on the website during the term of membership. It will be held in the members directory and current version of the members database for six months after membership lapses (to allow for late renewals) and securely archived in an encrypted backup of our database for a further period of 6 years to comply with our audit and HMRC rules, after which it will be permanently deleted.

16. Document owner

The Data Controller is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated October 2018 is available to all personnel of Voluntary Sector Studies Network on the corporate intranet.

This policy document was approved by VSSN's Steering Group and is issued by the Chair on a version controlled basis.

Name of Chair: Dr Angela Ellis Paine Date: 22 October 2018

Change history record

Issue	Description of Change	Approval	Date of Issue
1	{{ insert_detail_of_change_1 }}	{{ insert_manager_name_1 }}	{{ insert_date_1 }}
2	{{ insert_detail_of_change_2 }}	{{ insert_manager_name_2 }}	{{ insert_date_2 }}

Appendix A

Definitions under the GDPR

- *Child* means anyone under the age of 16. It is only lawful to process the personal data of a child under the age of 13 upon receipt of consent from the child's parent or legal custodian.

- *Data controller* may be a natural or legal person, whether a public authority, agency or other body which, individually or jointly with others, is in charge of ascertaining the purposes and means by which personal data shall be processed. Where EU or Member State law predetermines the purposes and means of processing personal data, the data controller or, if appropriate, the specific criteria for selecting the data controller, may be provided for by EU or Member State law.

- *Data subject* refers to any living person who is the subject of personal data (see below for the definition of 'personal data') held by an organisation. A data subject must be identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, mental, economic or social.

- *Data subject consent* refers to any specific indication by the data subject that signifies consent to the processing of personal data. Consent may take place by way of a written or oral statement or by clear, unambiguous action and must be given freely at all times, without duress, with the data subject being properly informed.

  Establishment refers to the administrative head office of the 'data controller' in the EU, where the main decisions regarding the purpose of its data processing activities are made.
- *Filing system* refers to any personal data set which is accessible on the basis of certain benchmarks, or norms and can be centralised, decentralised or dispersed across various locations.

- *Personal data* – means any information relating to a data subject.

- *Personal data breach* refers to a security breach which results in the disclosure, alteration, destruction or loss of personal data, as well as unauthorised access to personal data that is stored, transmitted or processed by any other means, whether accidentally or unlawfully. All personal data breaches must be reported to relevant regulatory authority by the 'data controller', whereas the data subject need only be informed of a data breach when it is likely that the breach will have an adverse effect on his or her privacy or personal data.

- *Processing* refers to any action taken in relation to personal data, including but not limited to collection, adaptation or alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise.

- *Profiling* refers to any form of personal data processing that is automated, with the intention of assessing personal aspects of a data subject or analysing a data subject's employment performance, economic status, whereabouts, health, personal preferences and behaviour. The data subject has a right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling.

- *Special categories of personal data* refers to personal data covering such matters as racial or ethnic origin, beliefs - whether religious, political or philosophical - membership of a trade-union and data relating to genetics, biometric identification, health, sexual orientation and sex life.

- *Territorial scope* the GDPR applies to all EU based 'data controllers' who engage in the processing of data subjects**'** personal data as well as to 'data controllers' located outside of the EU that process data subjects**'** personal data so as to provide goods and services, or to monitor EU based data subject behaviour.

- *Third party* is a natural or legal person other than the data subject who is authorised to process personal data, whether a public authority, agency or other body controller, processor or any other person(s) under the direct authority of the controller or processor.