DATA PROTECTION POLICY

Dates:
Date of Policy: February 2013
Date of last policy review: July 2021
Date of next policy review: July 2022

Related Policies: Safeguarding Policy, Company Handbook, Data Retention Policy, Risk Management Policy

1. Introduction

1.1 This Policy sets out the obligations of YSS regarding data protection and the rights of its employees, volunteers, service users in respect of their personal data under Data Protection Law. "Data Protection Law" means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

1.2 This Policy sets out YSS' obligations regarding the collection, processing, transfer, storage, and disposal of personal data relating to data subjects. The procedures and principles set out herein must be followed at all times by YSS, its employees, agents, contractors, and other parties working on behalf of YSS.

2. General Provisions

2.1 YSS needs to collect and use certain types of information about the people we work with in order to operate. These include current, past and prospective service users, past and present employees, suppliers and others with whom we conduct business.

2.2 In addition, YSS may occasionally be required by law to collect and use certain types of information to comply with the requirements of partner agencies. This personal information must be dealt with properly however it is collected, recorded and used.

2.3 This policy applies to all personal data collected and processed by YSS.

2.4 The Responsible Person referred to as the Data Protection Officer shall take responsibility for YSS' ongoing compliance with this policy and will report to the Board of Trustees.

2.5 This policy shall be reviewed at least annually.

2.6 YSS shall maintain its registration with the Information Commissioner's Office as an organisation that processes personal data.

3. **Definitions**

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
"data controller"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, YSS is the data controller of all personal data relating to data subjects;
"data processor"	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
"data subject"	means a living, identified, or identifiable natural person about whom YSS holds personal data;
"EEA"	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
"personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
"personal data breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"pseudonymisation"	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual

orientation, biometric, health and criminal record or genetic data.

4. **Scope**

4.1 YSS is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it works.

4.2 YSS' Data Protection Officer is Anna Wykurz, Director of Finance and Resources, datamanager@yss.org.uk The Data Protection Officer is responsible for working together with the Senior Management Team (SMT) and HR & Governance Coordinator for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

4.3 All members of SMT and line managers are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of YSS comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

4.4 Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;

b) if consent is being relied upon in order to collect, hold, and process personal data;

c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;

d) if any new or amended privacy notices or similar privacy-related documentation are required;

e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);

f) if a personal data breach (suspected or actual) has occurred;

g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;

h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

i) if personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so;

j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;

k) when personal data is to be used for purposes different to those for which it was originally collected;

l) if any automated processing, including profiling or automated decision-making, is to be carried out; or

m) if any assistance is required in complying with the law applicable to direct marketing.

5. The Data Protection Principles

5.1 YSS is committed to processing data in accordance with its responsibilities under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The UK GDPR sets out the following principles with which anyone handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed 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.

6. The Rights of Data Subjects

The UK GDPR sets out the following key rights applicable to data subjects:

6.1 the right to be informed;

6.2 the right of access;

6.3 the right to rectification;

6.4 the right to erasure (also known as the 'right to be forgotten');

6.5 the right to restrict processing;

6.6 the right to data portability;

6.7 the right to object; and

6.8 rights with respect to automated decision-making and profiling.

7. Lawful, Fair, and Transparent Data Processing

7.1 Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful only if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7.2 If the personal data in question is special category personal data (also known as 'sensitive personal data') at least one of the following conditions must be met in addition to one of the conditions set out above:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);

b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject;

c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) the processing relates to personal data which is manifestly made public by the data subject;

e) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

f) the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

g) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;

h) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

i) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

7.3 Additionally, specific and up-to-date guidance on handling Criminal Offence data can be accessed via this link.

8. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing any personal data, the following shall apply:

8.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

8.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

8.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

8.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

8.5 Where special category personal data is processed, YSS shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

8.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that YSS can demonstrate its compliance with consent requirements.

9. Adequate, Relevant, and Limited Data Processing

9.1 YSS shall only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above.

9.2 Employees, agents, contractors, or other parties working on behalf of YSS may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

9.3 Employees, agents, contractors, or other parties working on behalf of YSS may process personal data only when the performance of their job duties requires it. Personal data held by YSS cannot be processed for any unrelated reasons.

10. Accuracy of Data and Keeping Data Up-to-Date

10.1 YSS shall ensure that all personal data collected, processed, and held by it is kept

accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 16, below.

10.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

10.3 It is the responsibility of every employee to ensure that the personal data they have provided to YSS about themselves as employees and other relevant data subjects is kept up-to-date. If any such personal data changes, employees should ensure that the relevant member of staff and/or department is informed as soon as is reasonably possible. YSS relies on the cooperation of its employees to help meet its obligations under Data Protection Law.

11. Data Retention

11.1 YSS shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which it was originally collected, held, and processed.

11.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it securely and without delay.

11.3 For full details of the YSS' approach to data retention, including retention periods for specific personal data types held by YSS, please refer to our Data Retention Policy.

12. Secure Processing

12.1 YSS shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

12.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

12.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b) authorised users must always be able to access personal data as required for the authorised purpose or purposes.

13. Accountability and Record-Keeping

13.1 YSS shall follow a 'privacy by design' approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 14 for further information).

13.2 All employees, agents, contractors, or other parties working on behalf of YSS shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable YSS policies.

13.3 YSS' data protection compliance shall be regularly reviewed and evaluated.

14. **Data Protection Impact Assessments and Privacy by Design**

14.1 In accordance with the 'privacy by design' principles, YSS shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

14.2 The principles of 'privacy by design' should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;

b) the state of the art of all relevant technical and organisational measures to be taken;

c) the cost of implementing such measures; and

d) the risks posed to data subjects and to YSS, including their likelihood and severity.

14.3 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

a) the type(s) of personal data that will be collected, held, and processed;

b) the purpose(s) for which personal data is to be used;

c) YSS' objectives;

d) how personal data is to be used;

e) the parties (internal and/or external) who are to be consulted;

f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

g) risks posed to data subjects;

h) risks posed both within and to YSS; and

i) proposed measures to minimise and handle identified risks.

15. **Keeping Data Subjects Informed (Privacy Notice)**

15.1 YSS shall provide the information set out in Part 15.2 to every data subject:

a) Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i) if the personal data is used to communicate with the data subject, when the first communication is made; or

ii) if the personal data is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

15.2 The following information shall be provided in the form of a privacy notice:

a) details of YSS including, but not limited to, all relevant contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;

b) the purpose(s) for which the personal data is being collected and will be processed and the lawful basis justifying that collection and processing;

c) where applicable, the legitimate interests upon which YSS is justifying its collection and processing of personal data;

d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) where the personal data is to be transferred to one or more third parties, details of those parties;

f) details of applicable data retention periods;

g) details of the data subject's rights under the UK GDPR;

h) details of the data subject's right to withdraw their consent to YSS' processing of their personal data at any time (where applicable);

i) details of the data subject's right to complain to the Information Commissioner's Office;

j) where the personal data is not obtained directly from the data subject, details about the source of that personal data;

k) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of personal data and details of any consequences of failing to provide it; and

l) details of any automated decision-making or profiling that will take place using personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

16. Data Subject Access

16.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which YSS holds about them, what it is doing with that personal data, and why.

16.2 Data Subjects wishing to make a SAR should do using a Subject Access Request Form (attached in Appendix A), sending the form to the YSS' Data Protection Officer at datamanager@yss.org.uk. The form is available on YSS' website and/or on request.

16.3 Responses to SARs must normally be made within one month of receipt; however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

16.4 All SARs received shall be handled by Data Protection Officer.

16.5 YSS does not charge a fee for the handling of normal SARs. YSS reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

17. Rectification of Personal Data

17.1 Data subjects have the right to require YSS to rectify any of their personal data that is inaccurate or incomplete.

17.2 YSS shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing YSS of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

17.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

18. Erasure of Personal Data

18.1 Data subjects have the right to request that YSS erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for YSS to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent (where applicable) to YSS's holding and processing their personal data;

c) the data subject objects to YSS holding and processing their personal data (and there is no overriding legitimate interest to allow YSS to continue doing so);

d) the personal data has been processed unlawfully;

18.2 Unless YSS has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

18.3 In the event that any personal data that is to be erased in response to an data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

19. Data Portability

19.1 To facilitate the right of data portability, YSS shall make available all applicable personal data to data subjects in the following formats:

a) Written document;

b) E-mail;

c) Electronic storage device (i.e. USB memory stick).

19.2 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

19.3 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

20. Equal Opportunities Monitoring Information

20.1 YSS collects, holds, and processes certain information for the purposes of monitoring equal opportunities. Some of the personal data collected for this purpose, such as details of ethnic origin and religious beliefs, falls within the UK GDPR's definition of special category data (see Part 3 of this Policy for a definition). Where possible, such data will be anonymised. Where special category personal data remains, it will be

collected, held, and processed strictly in accordance with the conditions for processing special category personal data, as set out in Part 7.2 of this Policy.

20.2 Non-Anonymised Equal opportunities monitoring information shall be accessible and used only by the relevant employees of YSS and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of YSS except in exceptional circumstances where it is necessary to protect the vital interests of the data subject(s) concerned, and such circumstances satisfy one or more of the conditions set out in Part 7.2 of this Policy.

20.3 Equal opportunities monitoring information will only be collected, held, and processed to the extent required to prevent, reduce, and stop unlawful discrimination in line with the Equality Act 2010.

20.4 All data subjects have the right to request that YSS does not keep equal opportunities monitoring information about them. All requests must be made in writing and addressed to Denise White, HR & Governance Coordinator.

21. Data Security - Transferring Personal Data and Communications

YSS shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

21.1 All emails containing personal data must be encrypted;

21.2 All emails containing personal data must be marked “confidential”;

21.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

21.4 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

21.5 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient;

21.6 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”;

22. Data Security - Storage

YSS shall ensure that the following measures are taken with respect to the storage of personal data:

22.1 All electronic copies of personal data should be stored securely and require using passwords and, where applicable, data encryption;

22.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

22.3 No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of YSS;

23. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer

to Data Retention Policy.

24. **Data Security - IT Security**

YSS shall ensure that the following measures are taken with respect to IT and information security:

24.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;

24.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of YSS, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method;

24.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date;

24.4 No software may be installed on any YSS owned computer or device without the prior approval of the Data Protection Officer;

25. **Data Security – Working from Home**

25.1 All YSS employees, agents, contractors, or other parties working on behalf of YSS must at all times ensure that access, sharing and transferring of any personal data physically kept outside YSS' premises (i.e. private home, car) complies with the same data security measures, as outlines in Parts 21 to 24. All electronic personal data must be password protected and encrypted, where applicable, and all hardcopy personal data must be kept in lockable storage, unless in transit, where physically supervised by (a) person(s) handling that personal data.

26. **Organisational Measures**

YSS shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

26.1 All employees, agents, contractors, or other parties working on behalf of YSS shall be made fully aware of both their individual responsibilities and YSS' responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;

26.2 Only employees, agents, contractors, or other parties working on behalf of YSS that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by YSS;

26.3 All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;

26.4 All employees, agents, contractors, or other parties working on behalf of YSS handling personal data will be appropriately trained to do so;

26.5 All employees, agents, contractors, or other parties working on behalf of YSS handling employee personal data will be appropriately supervised;

26.6 All employees, agents, contractors, or other parties working on behalf of YSS handling personal data shall be required and encouraged to exercise care, caution, and

discretion when discussing work-related matters, whether in the workplace or otherwise;

26.7 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

26.8 All personal data held by YSS shall be reviewed periodically, as set out in the Data Retention Policy;

26.9 The performance of those employees, agents, contractors, or other parties working on behalf of YSS handling personal data shall be regularly evaluated and reviewed;

26.10 All agents, contractors, or other parties working on behalf of YSS handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of YSS arising out of this Policy and Data Protection Law;

26.11 Where any agent, contractor or other party working on behalf of YSS handling personal data fails in their obligations under this Policy, that party shall indemnify and hold harmless YSS against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

27. Sharing Personal Data

27.1 YSS may only share personal data with third parties if specific safeguards are in place YSS will adhere at all times to the Data Sharing Code of Practice, which can be accessed from ICO website: https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/

27.2 Personal data may only be shared with other employees, agents, contractors, or other parties working on behalf of YSS if the recipient has a legitimate, job-related need-to-know.

27.3 Where a third-party data processor is used, that processor shall process personal data on behalf of YSS (as data controller) only on the written instruction of YSS.

27.4 Personal data may only be shared with third parties in the following circumstances:

a) the third party has a legitimate need to know the information for the purpose of providing services to YSS and/or YSS' service users;

b) the sharing of the personal data concerned complies with the privacy notice provided to the affected data subjects;

c) the third-party recipient has agreed to comply with all applicable data security standards, policies, and procedures, and has put in place adequate security measures to protect the personal data;

d) (where applicable) the transfer complies with any cross-border transfer restrictions;

28. Data Breach Notification

28.1 All personal data breaches must be reported immediately to the Data Protection Officer.

28.2 If an employee, agent, contractor, or other party working on behalf of YSS becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

28.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

28.4 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 27.3) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

28.5 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the YSS' Data Protection Officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by YSS to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

29. Implementation of Policy

This Policy shall be deemed effective as of 21 July 2021 No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Policy Review Assessment

Policy Title	***YSS DATA PROTECTION POLICY***
Review/New	*review*
Date	*20/07/2021*
Reason for Review/Creation of Policy	*Policy was scheduled for a review.*
Resource Implications	*none*
Impact on other areas of the charity	*All YSS colleagues and Trustees need to familiarise themselves and adhere to the policy. The policy brings together more elements such as guidelines on sharing and storage of personal data, ICT security and privacy by design – in line with YSS Digital Strategy. It also now consists of the Subject Access Request procedure, which previously was not included in Data Protection Policy. It now also refers to risk management by outlining YSS' measures and obligations with respect to personal data processing, staff training and staff responsibilities.*

Appendix A

YSS
Subject Access Request Form

The following information is required to help YSS to respond fully to your request. Please complete the information below and return this form by either post to Data Protection Officer, Polysec House, Blackpole Trading Estate West, Hindlip Lane, Worcester, WR3 8TJ or e-mail datamanager@yss.or.uk. Please allow one month for a response.

Your details

Title:	
Forename(s):	
Surname:	
Address:	
Telephone number:	
Email:	

Information being requested

Please provide specific details (and any relevant dates) of the information being requested and any additional information that may enable us to locate your personal data.

By completing this form, you are making a request under the UK GDPR for information held about you by YSS that you are entitled to receive.

Declaration

By signing below, you confirm that you are the Data Subject named in this Subject Access Request Form. You warrant that you are the individual named and will fully indemnify YSS for all losses and expenses incurred if you are not. YSS cannot accept requests in respect of your personal data from anyone else, including members of your family. YSS reserves the right to take all reasonable steps in order to verify your identity for the purpose of releasing any personal data information with you.

Your Name:	
Signature:	
Date:	