Data Protection & GDPR Policy

TABLE OF CONTENTS

1.	Introduction	Pg. 3
2.	Principles and Legal Framework	3
3.	Policy Review	3
4.	Termnology	3
5.	Policy Statement	4
6.	Responsibilities	4
7.	Data Protection Officer	4
8.	Lawful Basis for Processing Personal Data	4
9.	Transparency	4
10.	Consent	4
11.	Data Security	4
12.	Retention Periods and Disposal of Personal Data	5
13.	Confidentality and Safeguarding Information Sharing	5
14	Working With Partner Organisations and Shared Systems	5
15.	Data Breaches	5
16.	Data Accuracy	5
17.	Direct Marketing	6
18.	Individuals' Rights and Subject Access Requests (SAR)	6
18.1	GDPR Rights	6
18.2	Access to Data	6
19.	Transfer Outside of the UK	6
20.	References	6
21.	Associated Lifespace Policies	6
Appendix 1	Privacy Notice	7
Appendix 2	Privancy Statement	10
Appendix 3	GDPR & Bring Your Own Device (BYOD) Employee/Vokunteer Understanding and Agreement Form	13

1. INTRODUCTION

The UK General Data Protection regulations (GDPR) and the Data Protection Act 2018 applies to organisations that process personal data. Lifespace Trust is a data controller for most of its work and may use data processors to support delivery of services. Lifespace will ensure appropriate written agreements are in place with any processors.T herefore this policy applies to all board members, staff, associates and volunteers and to any third party processing personal data on behalf of Lifespace.

The purpose of this policy is to enable Lifespace to:

- Comply with the law in respect of the data it holds about individuals;
- Follow good practice;
- Protect Lifespace's young people, trustees, staff, volunteers and other individuals;
- Reduce the likelihood, and potential impact of, a breach of its responsibilities.

2. PRINCIPLES AND LEGAL FRAMEWORK

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

Lifespace will process personal data in line with the UK GDPR principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability.

Lifespace will be able to demonstrate compliance through appropriate records, training, procedures and governance.

3. POLICY REVIEW

The policy will be reviewed every three years by the Data Protection Officer with final approval by the Board of Trustees. It will also be reviewed in response to changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness.

4. TERMINOLOGY

This **"Data"** is information which is stored electronically, on a computer, or in certain paper based filing systems. This includes photographic images and video footage.

"Data subjects" are all living individuals about whom we hold and process personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

"Personal data" means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address telephone or date of birth) or it can be an opinion (such as from a questionnaire).

"Special Category data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data; biometric data processed for the purpose of uniquely identifying an individual; data concerning health; or data concerning a person's sex life or sexual orientation. Processing special category data requires both a lawful basis under Article 6 UK GDPR and a condition under Article 9 UK GDPR, together with a condition under the Data Protection Act 2018 where required. Consent is one possible condition, but other conditions may apply, including in relation to safeguarding and child protection. Criminal offence data is not special category data and is subject to the separate requirements applying to criminal offence data.

"Data controllers" are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act.

"Data Protection Officer" is the name given to the person in an organisation who is the central point of contact for all data compliance issues.

"Data processors" include any person who processes personal data on behalf of a data controller.

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

5. POLICY STATEMENT

Lifespace will comply with the UK GDPR and the Data Protection Act 2018, follow good practice, respect individuals' rights, and be open and transparent about how personal data is used.

We will apply privacy by design and default, limit access to personal data on a need-to-know basis, keep data secure, and ensure staff and volunteers receive appropriate induction and refresher training.

Where processing is likely to result in a high risk to individuals (for example, large-scale processing of special category data), Lifespace will undertake a Data Protection Impact Assessment (DPIA) and record decisions.

6. RESPONSIBILITIES

The Board recognises its overall responsibility for ensuring that Lifespace complies with its legal obligations.

All staff and volunteers must follow Lifespace procedures for handling personal data, report concerns and incidents promptly, and complete required training.

7. DATA PROTECTION OFFICER

Lifespace's Data Protection Lead (currently the Chief Executive) is the central point of contact for data protection compliance, including oversight of policies, training, incident management and subject access requests.

The Data Protection Lead will maintain an incident/breach log, oversee DPIAs where needed, and ensure appropriate contractual clauses are in place with processors.

Significant breaches of this policy will be handled under Lifespace's *Disciplinary Policy*.

8. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

Lifespace will identify and document a lawful basis for each processing activity under Article 6 UK GDPR. Where special category data is processed, Lifespace will also identify and document an applicable Article 9 condition and, where relevant, a condition under Schedule 1 of the Data Protection Act 2018. Where a Schedule 1 condition requires an Appropriate Policy Document, Lifespace will maintain that document and the associated record of processing, including how the data protection principles and retention and deletion requirements are met.

Lifespace's processing register will distinguish referral and assessment, routine mentoring and session records, safeguarding activity, service evaluation, and workforce administration. For each purpose, it will record the applicable Article 6 lawful basis and, where relevant, the Article 9 and DPA 2018 Schedule 1 conditions, together with the retention arrangements and supporting documentation.

9. TRANSPARENCY

Lifespace will provide clear privacy information explaining what data we collect, why, who we share it with, how long we keep it, and how individuals can exercise their rights.

10. CONSENT

Where Lifespace relies on consent, it will be freely given, specific, informed and unambiguous, and individuals will be able to withdraw consent. Lifespace will record consent decisions.

Consent is not required where another lawful basis applies. In particular, for safeguarding and child protection matters, Lifespace will not rely on consent where seeking it could increase risk, undermine safeguarding, or delay protective action.

11. DATA SECURITY

Lifespace will take appropriate technical and organisational measures to protect personal data from unauthorised access, loss, alteration, disclosure or destruction. Measures include access controls and least privilege, strong authentication (including MFA where available), secure storage, secure transfer methods, and secure disposal of paper and devices.

Staff and volunteers must follow Lifespace guidance on secure working, including remote working and use of personal devices, and must report any suspected incident immediately.

12. RETENTION PERIODS AND THE DISPOSAL OF PERSONAL DATA

Lifespace holds a retention and disposal schedule that sets out how long we keep different categories of of records are kept. Personal data will be kept only as long as needed for the purpose collected, legal/regulatory requirements, safeguarding, and audit/complaints, and will be securely deleted or destroyed when no longer required.

13. CONFIDENTIALITY AND SAFEGUARDING INFORMATION SHARING

Lifespace respects confidentiality and will share personal data only where there is a lawful basis and it is necessary and proportionate.

Safeguarding: The UK GDPR and the Data Protection Act 2018 do not prevent Lifespace from sharing information where it is necessary to safeguard children and promote their welfare. Where there is a safeguarding concern, relevant information will be shared promptly and appropriately with safeguarding leads and relevant agencies on a need-to-know basis. Wherever it is practicable and safe, Lifespace will be transparent with the child and/or carers about what is being shared and why; however, consent is not required where seeking it would increase risk or delay action.

14. WORKING WITH PARTNER ORGANISATIONS AND SHARED SYSTEMS

Lifespace works in partnership with other organisations, including schools, local authorities, health services and voluntary sector partners, to deliver safe and effective support for children and young people.

Where Lifespace shares personal data with partner organisations, or where Lifespace staff access or use a third-party database or information system, this will be governed by an appropriate Information Sharing Agreement (ISA) and/or Memorandum of Understanding (MOU). These agreements set out:

- the purpose and lawful basis for sharing;
- the roles and responsibilities of each organisation (including controller or processor status);
- security arrangements and access controls;
- retention and disposal arrangements; and
- procedures for incidents, breaches and subject access requests.

Information will be shared lawfully, proportionately and on a need-to-know basis.

Safeguarding: The UK GDPR and the Data Protection Act 2018 do not prevent Lifespace from sharing information where it is necessary to safeguard children and promote their welfare. Where there is a safeguarding concern, information may be shared with relevant partner organisations without consent where seeking consent could increase risk or delay protective action.

Lifespace will ensure staff are trained and supported to understand when and how information can be shared appropriately in partnership contexts.

15. DATA BREACHES

All staff and volunteers must report suspected data incidents immediately to their line manager and the Data Protection Lead.

Lifespace will assess the risk posed by any personal data breach. Where required, Lifespace will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of a notifiable breach, and where there is a high risk to individuals, Lifespace will also inform affected individuals without undue delay. Lifespace will keep a record of all breaches and decisions, whether or not they are reported externally.

16. DATA ACCURACY

Lifespace will take reasonable steps to ensure personal data is accurate and kept up to date. Individuals can request correction of inaccurate data.

17. DIRECT MARKETING

Lifespace will only send marketing/fundraising communications in line with data protection law and, where relevant, the Privacy and Electronic Communications Regulations (PECR). Individuals will be offered clear choices and easy opt-out mechanisms, and preferences will be recorded.

18. INDIVIDUALS' RIGHTS AND SUBJECT ACCESS REQUESTS (SAR)

18.1 GDPR RIGHTS

Individuals have the following rights under GDPR:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

In relation to exercising these rights, any individual can request to see what information Lifespace holds about them through a 'subject access request', and to request that that information is rectified, erased or restricted If Lifespace does not have an overriding lawful purpose for retaining that information, for example, because it relates to a safeguarding concern.

18.2 ACCESS TO DATA

Individuals have rights under the UK GDPR, including the right to be informed, access, rectification, erasure, restriction, portability, objection, and rights relating to automated decision-making.

SARs should be made in writing. Lifespace will verify identity where necessary and respond within one month (or within an extended period where lawful and communicated). Lifespace will redact third-party data where appropriate and will consider exemptions on a case-by-case basis, documenting any decision to withhold or limit information, including where disclosure may risk serious harm or prejudice safeguarding/child protection processes.

19. TRANSFERS OUTSIDE THE UK

Lifespace does not routinely transfer personal data outside the UK. Where an international transfer is necessary, Lifespace will ensure an appropriate safeguard is in place (for example, adequacy regulations or standard contractual clauses), as required by law.

20. REFERENCES

This policy references:

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

21. RELATED LIFESPACE POLICIES

- Disciplinary Policy
- Complaints Policy
- Confidentiality Policy
- Information Technology Policy
- Staff Behaviour ("Code of Conduct") Policy
- Safeguarding and Child Protection Policy

APPENDIX 1:

Subject Access Request

When submitting a Subject Access Request under the Data Protection Act 2018, Lifespace has one calendar month to release your information. This period begins once the Data Protection Officer receives your request, along with valid proof of your identity.

The information you provide on this form will allow us to identify where the information that you have requested may be located. Please provide as much detail as possible when submitting your request. We may contact you for further clarification, if necessary.

SECTION 1:

Are you the Data Subject? (The individual who is the subject of the required information). Please tick the appropriate box.

☐ I **AM** the Data Subject and enclose evidence of my identity e.g. photocopy of driving license, birth certificate, passport or marriage certificate.

☐ I am **NOT** the Data Subject, but I am acting on their behalf. I have written authority, which I enclose and evidence of their identify e.g. photocopy of their driving licence, birth certificate or passport.

☐ I am **NOT** the Data Subject, but I am acting on their behalf as their parent or legal guardian and enclose evidence of their identity e.g. photocopy of birth certificate, passport.

SECTION 2: DETAILS OF THE DATA SUBJECT

Full name	
Former name(s)	
Current address (including postcode)	
Former address(s)	
Date of birth	
Contact telephone number (including area code)	
Email address	
Any additional information that may help identify your relationship with Lifespace	

SECTION 4: INFORMATION ABOUT YOUR REQUEST

Describe the information you are requesting in as much detail as possible. Where possible, please provide the details of relevant names, dates and/or projects/services at Lifespace. This will enable us to access and release your information more promptly.	
Signature	
Date	
How would you like the information to be released to you? Please tick	Hard Copy (by post): ☐ Electronic copy – PDF. (by email): ☐ (Hard Copy) Collect in person: ☐

Please return this form either by email to lisa.carroll@lifespace.org.uk or at the following address: Lisa Carroll, Chief Executive, Tyler House, Tyler Street, Stratford-Upon-Avon, Warwickshire, CV37 6TY

SECTION 5: IDENTIFICATION OF PERSON REQUESTING A SUBJECT ACCESS REQUEST

Document(s) viewed (e.g passport)	Date of checking	Signature of DPO at Lifespace

HOW LIFESPACE WILL COLLATE THE INFORMATION

Once the information you have requested has been confirmed, we will begin the process of contacting colleagues across Lifespace and collating the information.

LIFESPACE WILL REVIEW YOUR INFORMATION

Before we release your information to you, it is very important that we review it to ensure that it does not contain the personal data of other individuals (third parties). All personal information of other individuals will be redacted (removed or blocked out), as it is not relevant to you. If we have had to redact information, then this will be drawn to your attention in the covering letter.

If your request contains a substantial amount of information (from various sources), then reviewing it can be time consuming. We review information as we receive it and aim to release it to you within one calendar month of the request being received and your identification confirmed. In exceptional circumstances where it is not possible to comply within this period you will be informed of the delay, the reason for the delay, and given a timescale for when your request is likely to be met.

In certain circumstances, Data Protection legislation may permit Lifespace to withhold information, for example if the information is likely to cause serious harm to the physical or mental health or condition of you, or any other person, and information relating to or provided by a third person who has not consented to the disclosure.

LIFESPACE WILL RELEASE YOUR INFORMATION

Once the information has been reviewed, we will contact you and confirm the details for releasing it to you. If you have requested that we provide your information electronically, this will be encrypted with a password. If you have requested that we send your information to you by post, then we will do so using Royal Mail 'Signed For' delivery.

If you have any queries regarding your requested information, then you will be able to raise these with us via admin@lifespace.org.uk

SECTION 6: WE DELETE YOUR INFORMATION

It is important that we do not retain your personal data for any longer than is necessary. Therefore, all of the information **collated as part of your SAR** will be deleted either 12 months after the release date, or 12 months after the last query you made regarding the request has been resolved; whichever is the later. Original copies of the requested information will remain where they were located and will be retained as per Lifespace's Data Retention schedule.

APPENDIX 2:

Privacy Notice

Lifespace is a Charity Registered in England (No. 1122170) and a Company Limited by Guarantee (No. 6428820). Lifespace manages and delivers a range of contracts and projects.

This privacy notice covers what we do with any information we collect about you when accessing the Lifespace website.

("We") are committed to protecting and respecting your privacy. This policy (together any other documents referred to on it) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it. The rules on processing of personal data are set out in the General Data Protection Regulation (the "GDPR").

1. DEFINITIONS

Data controller - A controller determines the purposes and means of processing personal data.
Data processor - A processor is responsible for processing personal data on behalf of a controller.
Data subject – Natural person

1.1 CATEGORIES OF DATA:

Personal data and special categories of personal data Personal data - The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier (as explained in Article 6 of GDPR). For example name, passport number, home address or private email address. Online identifiers include IP addresses and cookies.

Special categories personal data - The GDPR refers to sensitive personal data as 'special categories of personal data' (as explained in Article 9 of GDPR). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Other examples include racial and ethnic origin, sexual orientation, health data, trade union membership, political opinions, religious or philosophical beliefs.

Processing - means any operation or set of operations which is performed on personal data or on 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.

Third party - means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

2. WHO ARE WE?

Lifespace Trust is the data controller. This means we decide how your personal data is processed and for what purposes. Our contact details are: Lifespace Trust, Tyler House, Tyler Street, Stratford-upon-Avon, Warwickshire CV37 6TY. For all data matters contact our data representative using the details above.

3. THE PURPOSE(S) OF PROCESSING YOUR PERSONAL DATA

We use your personal data for the following purpose: To deliver safe and effective mentoring services to children and young people to help them reduce distress, build resilience and achieve more.

4. THE CATEGORIES OF PERSONAL DATA CONCERNED

With reference to the categories of personal data described in the definitions section, we process the following categories of your data:

- Personal data (for example, your name, gender, date of birth, school/college (if applicable))
- Special categories of data (for example, information about your physical or mental health if supplied to us by you or by the person or organisation that requested mentoring for you.)

We have obtained your personal data from the mentoring request form completed by the person or organisation that requested mentoring for you and, once mentoring has started, from you during mentoring sessions.

5. WHAT IS OUR LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA?

a. **General personal data — Article 6 UK GDPR**
We process general personal information where necessary for our legitimate interests in delivering safe and effective mentoring services to children and young people, helping them reduce distress, build resilience and achieve more. We balance these interests against your interests, rights and freedoms, giving particular consideration to children's privacy.

b. **Routine mentoring:** Where we receive or record special category information as part of a referral or the delivery of mentoring, we will identify and document the appropriate Article 9 UK GDPR condition for that processing. Where we rely on explicit consent, this will meet the requirements of Article 9(2)(a) UK GDPR.

c. **Safeguarding and child protection:** Where processing is necessary for substantial public-interest safeguarding purposes, we may rely on Article 9(2)(g) UK GDPR together with Schedule 1, Part 2, paragraph 18 of the Data Protection Act 2018, where its requirements are met. This includes circumstances where consent cannot be given, cannot reasonably be obtained, or seeking consent would prejudice the protection being provided.

6. Sharing your personal data
Your personal data will be treated as strictly confidential, and will be shared only with your Lifespace mentor and, if required to facilitate delivery of a safe and effective mentoring services, our small administrative team.

7. How long do we keep your personal data?
We keep your personal data for no longer than reasonably necessary and we only retain your data either in limited form to record that you received a service from us or in more detailed form in the case of any legal claims/complaints or child protection purposes etc.

8. Providing us with your personal data
You are under no statutory or contractual requirement or obligation to provide us with your personal data but failure to do so could result in us not offering a mentoring service to you or stopping an existing mentoring service.

9. Your rights and your personal data
Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data:

- The right to request a copy of the personal data which we hold about you;
- The right to request that we correct any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary to retain such data;
- The right to withdraw your consent to the processing at any time, where consent was your lawful basis for processing the data;
- The right to request that we provide you with your personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable i.e. where the processing is based on consent or is necessary for the performance of a contract with the data subject and where the data controller processes the data by automated means);
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable i.e. where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics).

10. Transfer of Data Abroad
We do not transfer personal data outside the EEA.

11. Automated Decision Making
We do not use any form of automated decision making in our business.

12. Further processing
If we wish to use your personal data for a new purpose, not covered by this Data Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions.

13. Changes to our privacy policy
Any changes we may make to our privacy policy in the future will be made available through our usual communication channels (e.g. our website) and, where appropriate, communicated directly to you.

14. How to make a complaint
To exercise all relevant rights, queries or complaints please in the first instance contact our data representative using the following contact details: Lifespace Trust, Tyler House, Tyler Street, Stratford-upon-Avon, Warwickshire CV37 6TY. If this does not resolve your complaint to your satisfaction, you have the right to lodge a complaint with

the Information Commissioners Office on 03031231113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England.

APPENDIX 3:

GDPR & Bring Your Own Device (BYOD) Employee/Volunteer Understanding and Agreement Form

Lifespace encourages all employees and volunteers to use Lifespace-issued devices wherever possible when accessing Lifespace systems, information or personal data. Where a colleague chooses to use their own personal device for Lifespace-related work, this should be done in line with the charity's Data Protection, Information Technology, Child Protection & Safeguarding and Confidentiality Policies and the guidance below. This helps protect company information, confidential records and personal data.

This agreement confirms that you understand and accept their your responsibilities when using a personally owned device to access, process, store or transmit company information and personal data.

Employee Responsibilities

I will protect company and personal data in accordance with GDPR and all company policies.

I will use strong passwords and keep my device protected with screen lock, encryption where available, and current security updates.

I will not share my device with unauthorised individuals while company information is accessible on the device.

I will immediately report any loss, theft, compromise, malware infection, or suspected data breach involving my device.

I will only access company systems using approved methods and applications.

GDPR Requirements

I understand that personal data must only be accessed for legitimate business purposes.

I will not copy, store, transfer, or share personal data unless authorised and necessary for my role.

I will dispose of or delete company data when no longer required instructed and in accordance with company retention requirements.

I understand that failure to comply may result in disciplinary action and may expose the company and individuals to regulatory penalties.

Company Rights

The company may remove company data from my device where necessary to protect business information or meet legal obligations. The company may require me to delete company information from my personal device, return or securely dispose of any company data.

The company may suspend or remove access to systems if security requirements are not met. where necessary to protect business information, personal data, or meet legal obligations.

Employee/Volunteer Declaration

I confirm that I have read, understood and agree to comply with the requirements set out in this document and all related company data protection, information security and BYOD policies.

Employee/Volunteer Name	
Job Title	
Signature	
Date	

This Policy is communicated to all staff, trustees suppliers and sub-contractors. It will be published on our website and made available to interested parties.

Date of Issue: October 2026	Signed: Lisa Carroll CEO
	Signed: Mark Beardmore Trustee (Governance & Compliance)
Date of Next Review:	October 2029
Policy Owner	Chief Executive Officer