The Springfield Project

Data Protection Policy

Policy information	
Organisation	The Springfield Project
Scope of policy	This policy applies to services where the Springfield Project is the Data Controller or the Data Processor. As Data Controller the Springfield Project will be processing (collecting, monitoring and retaining) data for its own purposes in order: to measure the efficiency of service delivery: to evidence equality and diversity; to measure impact and the effectiveness of our work; and to use for a wide range of publicity and we will be seeking consent to do this. As data processor we will be gathering evidence on behalf of funders and contractors where the lawful basis for gathering this data is to fulfil a contract. There may also be times when we are required to process information in order to comply with the law. This policy applies to anyone working with personal data that is controlled or processed by or on behalf of the Springfield Project including, and not limited to, service users, staff, volunteers and other individuals. It explains how the Springfield Project will hold and process personal data; the rights of a data subject and our obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Springfield Project. This policy is to be read in conjunction with: • Data Sharing and Confidentiality Policy • Data Security Policy • The Data Retention Policy • Subject Access Request Policy • Data Breach Policy • HR Data Protection Policy (in staff handbook)
Introduction	
Purpose of policy	The Springfield Project takes the security and privacy of everyone's data seriously. We need to gather and use information or 'data' about service users, staff, volunteers, apprentices, trainees, work placements and other individuals as part of our business. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the UK General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify everyone affected of the information contained in this policy. This policy will protect the organisation by explaining how we will comply with the law, follow best practice and protect our service users, staff, volunteers, apprentices, trainees, work placements and other individuals. In the rest of this document all individuals except service users will be referred to collectively as 'staff and volunteers'.
Brief introduction to	The Data Protection Act 1998 (DPA) defines the ways in which information about living people may be processed. The main intent is to protect individuals against misuse or abuse of information about them.

Data Protection Act 1998	
Data Protection Principles	The Springfield Project will comply with the GDPR seven key principles and ensure that personal data is: • Processed fairly and lawfully and in a transparent manner • Obtained for one or more specified, explicit and lawful purposes • Adequate, relevant and only limited to what is required • Accurate and where necessary kept up to date • Not kept in a form which permits identification of data subjects for longer than is necessary • Processed in accordance with the rights of data subjects • Processed in a manner that ensures appropriate security of the personal data.
Personal data	Personal information means any data or information, in paper or digital format, relating to a living individual who can be identified from that data. It does not include anonymised data. This policy applies to all data whether stored electronically or on paper. Personal data may have been shared with the Springfield Project by a fellow professional, or it could have been created by the Springfield Project.
Policy statement	The Springfield Project is required to process relevant personal data regarding members of staff, volunteers and a range of service users. This policy sets out our commitment to protecting all personal data and how we will ensure that staff understand how to handle data they have access to as part of their work. The Springfield Project will comply with both the law and good practice; we are committed to respecting individuals' rights. We will be open and honest with individuals whose data is held. We will provide training and support for staff and volunteers who handle personal data, so they can act confidently and consistently. We will notify the Information Commissioner voluntarily should there be a breach.
Key risks	The main risks to the organisation identified are: • information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information • individuals being harmed through data being inaccurate or insufficient • resulting reputational damage • resulting financial impact To mitigate this we will: • Appoint a named Data Protection Manager • Staff will read and sign the Data Protection policy to demonstrate understanding and compliance • Train key staff in data protection rules • Review policies and procedures in light of GDPR
Responsibilities	
Trustees	The trustees have overall responsibility for ensuring that the organisation complies with its legal obligations.

Data Protection Manager	The Data Protection Manager is the Chief Operating Officer The responsibilities include: • Briefing the CEO on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on Data Protection issues • Ensuring that Data Protection induction and training takes place • Handling subject access requests • Approving disclosures of personal data • Approving contracts with Data Processors
Specific other responsibilities	<u>Electronic Data Security</u> The Data Protection Manager is responsible for: • Physical locations of electronic equipment and portable storage. • Approving Data-Protection-related statements on publicity materials, letters, forms etc. • Adequate and appropriate of back up of electronic data. <u>Paper Data Security</u> The Data Protection Manager along with Managers is responsible for: • Physical location of paper files, case files, materials, letters, forms etc
Team/ Department managers	All Managers are responsible for implementing compliance in their areas and ensuring staff understand their responsibilities. Each department where personal data is handled will be responsible for ensuring good Data Protection practice is established and followed, and where required, drawing up their own operational procedures. The Data Protection Manager will be responsible for ensuring induction and training takes place. The departmental managers will ensure that the Data Protection Manager is informed of any changes in their uses of personal data that might affect the organisation's procedures.
Staff & volunteers	All staff and volunteers should read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.
Enforcement	Serious breaches of this policy caused by deliberate, negligent or reckless behaviour will result in disciplinary action and may even lead to criminal prosecution.
How data is processed	
Definitions	**1 How we define personal data** 1.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

Procedure	1.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials. 1.3 This personal data might be provided to us by individuals themselves, or someone else or it could be created by us. 1.4 We will collect and use the following types of personal data: • contact details and date of birth; • gender; • marital status and family details; • family circumstances; • other private matters relating to individuals and their families; • images (whether captured on CCTV, by photograph or video); • any other category of personal data which we may give notice of. • Information about any criminal convictions and offences. **2 How we define special categories of personal data** 2.1 '**Special categories of personal data**' are types of personal data consisting of information as to: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • genetic or biometric data; • health; and • sex life and sexual orientation. We may hold and use any of these special categories of personal data in accordance with the law. **3 How we define processing** 3.1 **'Processing'** means any operation which is performed on personal data such as: • collection, recording, organisation, structuring or storage; • adaption or alteration; • retrieval, consultation or use; • disclosure by transmission, dissemination or otherwise making available; • alignment or combination; and • restriction, destruction or erasure. This includes processing personal data which forms part of a filing system and any automated processing. Data subjects will be informed that their personal data is being collected, why and how it will be used. They will be informed on what lawful basis their data is being collected. Relevant privacy notices are available on the website and displayed on noticed boards in the welcome area. This policy will be made available to all staff and service users through: • the application process for staff and volunteers • registration or enrolment for service users • the initial meeting with service users • the website
Responsibility	It is the responsibility of all staff to ensure effective and timely communication with service users but the responsibility of the managers, in particular the Data Protection Manager, to ensure that the systems work and the information given to service users is

	current. All staff should be vigilant of areas of weakness and room for improvement and escalate such matters to the Data Protection Manager.
The legal process for processing data	
Underlying principles	**1 How will we process personal data?** 1.1 The Springfield Project will process personal data (including special categories of personal data) in accordance with our obligations under the DPA. 1.2 We will use personal data for: • if you give us our consent; • for complying with any legal obligation; • to fulfil a contract or • if it is necessary for our legitimate interests (or for the legitimate interests of someone else). We will not use personal data for an unrelated purpose without telling the individual concerned about it and telling them the legal basis that we intend to rely on for processing it. **2 Examples of when we might process personal data** 2.1 When we process special categories of personal data we will usually ask for your consent. We do not need consent to process special categories of personal data when we are processing it for the following purposes, which we may do: • where it is necessary for carrying out rights and obligations under law; • where it is necessary to protect an individual's vital interests or those of another person where they are physically or legally incapable of giving consent; • where the individual has made the data public; or • where processing is necessary for the establishment, exercise or defence of legal claims; and 2.3 We have to process personal data in various situations, for example: • to monitor and protect the health and safety of individuals, and third parties*; • monitoring compliance by us with our contractual obligations*; • to comply with laws which affect us*; • the prevention and detection of fraud or other criminal offences; • for any other reason which we may give notice of. 2.4 We will only process special categories of personal data in certain situations in accordance with the law. For example, in some circumstances we will only process personal data with explicit consent. If we asked for consent to process a special category of personal data then we would explain the reasons for our request. Individuals do not need to consent and can withdraw consent later if they choose by contacting the Springfield Project Admin Manager. *We do not take automated decisions about individuals using personal data or use profiling.
Privacy Notices	The Springfield Project must provide a Privacy Notice to service users to explain the legal basis which we use to process data. Where the service that we are delivering is contracted by another organisation, then the Privacy Notice relied upon for that work may be that of the contracting organisation. The relevant Privacy Notice will be shared with service users. Where service users access more than one service from the Springfield Project then two different Privacy Notices may apply. This will be explained to service users.

Forms of consent	Where consent is the legal basis for processing data, consent to holding personal data may be given verbally or in writing. Where possible it should be obtained in writing.
Opting out	Even where the organisation is not relying on consent, it may wish to give people the opportunity to opt out of their data being used in particular ways (in addition to the right to opt out of direct marketing — see below).
Withdrawing consent	The Springfield Project acknowledges that, once given, consent can be withdrawn, but not retrospectively. Sometimes we have no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn i.e. where a safeguarding incident has taken place. If a service user wishes to withdraw consent they must apply in writing to the Data Protection Manager.
Direct marketing	
Underlying principles	The Springfield Project will not hold personal data with the intention of cold mailing/calling service users. Consent will be sought to ensure we are able to keep in contact with service users to ensure they are up to date with the children's centre offer, and other activities on site, to offer invitations to events and to share news. This is in addition to any other lawful basis for holding personal data.
Opting out	Service users will not have to opt out of allowing contact for marketing purposes because the Springfield Project will not hold their data for this purpose.
Sharing lists	The Springfield Project will not share, give away or sell personal data for the purposes of facilitating marketing opportunities to a third party.
Electronic contact	Because of the Data Protection and Privacy Regulations 2003 most electronic marketing (by phone, fax, e-mail or text message) requires consent in advance. The Springfield Project seek consent to sell, share or give away personal data for the purposes of marketing in whatever format.
Staff training & acceptance of responsibilities	
Induction	All staff who have access to any kind of personal data will be told their responsibilities during their induction procedures.
Continuing training	There will be opportunities to raise Data Protection issues during staff training, team meetings, supervisions, etc. Regular training sessions will be offered to ensure staff are current in their knowledge.
Procedure for staff signifying acceptance of policy	Staff will be required to read a copy of this policy (which is available electronically on Breathe). GDPR training records will be stored on Skillgate. Any additional training will be added to training to staff records on Breathe.

Policy approved: March 2023
Policy reviewed: March 2026

Responsibility	The Data Protection Manager
Procedure	In partnership with the Board of Trustees.
Timing	Next review March 2029 unless legislation changes