Springboard

Privacy Notice Formerly known as Fair Processing Notice

Version 4 dated 18.01.2023

Springboard Chippenham are committed to protecting and respecting your privacy.

(The information Springboard Chippenham collects, holds and stores)

This policy, together with any other documents referred to in 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 practices **regarding your personal data and how we will treat it.**

This policy meets the requirements of both the Data Protection Act (DPA) 1998 and the GDPR (General Data Protection Regulations) 2018. It is based upon guidance published by the Information Commissioners Office (https://ico.org.uk/) the UK's Regulatory body.

Data Controller
As Springboard processes personal data relating to its children, families, staff, volunteers and visitors, Springboard is defined as a Data Controller for the purposes of the Data Protection Act.

Data Protection Principles

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall only be obtained for one or more lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and where necessary up to date
- Personal data shall not be kept longer than guidelines state
- Personal data shall be processed in accordance with the rights of the data subjects under the Data Protection Act 1998 and the General Data Protection Regulations, 2018
- Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data
- Personal data shall not be transferred to a country or territory outside of the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

Roles & responsibilities
The Springboard Management committee has the responsibility of ensuring that Springboard complies with the obligations under the Data Protection Act 1998.

Springboard

Day to day responsibilities lie with the Manager and the Data Protection Officer, who act on behalf of the Management Committee. They ensure all staff are aware of their data protection obligations and oversee any queries related to the storing and processing of personal data.
Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy.

Privacy/ fair processing notice
Springboard has a separate child privacy notice for children over the age of 13.

Data that Springboard holds includes:

- Personal data- name, address, contact information. (Data from which a person can be identified).
- Child's diagnosis, health, medical and developmental information.
- Some data defined as 'special classes'- these include ethnicity, genetic information (diagnosis) and medical conditions/ health information.

Why do we have to process data at Springboard?

- To support a child's development
- Monitor and report on a child's progress
- Provide appropriate support and care
- Assess how well we are doing as a setting

This information includes a child's contact details, assessment results and personal characteristics such as ethnicity, special educational needs, and any relevant medical information.

We may also receive information about the children from other organisations including, but not limited to other schools, Wiltshire Council (Local authority) and the Department for Education (DfE). Springboard will only retain the data it receives for as long as necessary to satisfy the purpose for which it has been collected.

Springboard will have access to the Family Information portal maintained by Wiltshire Council for the purpose of collating the parent and child information to claim the Early Years Entitlement funding. Parents will also have access to the portal.

We will not give or share information about an individual to anyone outside of Springboard without prior consent unless the law dictates and information sharing protocols require us to.

We are required by law to pass some of a child's information to the Local Authority and the Department for Education (DfE)

There are six lawful legal reasons for processing data. Springboard processes data from the following four categories:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose. This could be the consent to take a photograph and to use the photograph in a defined way.

(b) Contract: the processing of data is necessary for a contract we have with the individual, for example a work experience or student placement

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations) for example the retaining of paperwork for the specified legal timeframes.

(d) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. For example, sending a newsletter to a past donor/ supporter.

Subject Access Request (SAR)
Under the Freedom of Information Act an individual can ask to have a copy of the information held on them/ their child. This is called a Subject Access Request (SAR) and should be made in writing to the manager or Springboard's Data Protection Officer- (DPO) Anne Farrell. Contact can be made by email business@springboardchippenham.co.uk or by calling 01249 657145. The written request should include a correspondence address, contact number, email address and details about the information requested. The information will be provided electronically unless a hard copy has been specifically requested. No charge will be made for the first copy. The documents will be provided within one calendar month. ID will need to be shown by the person making the SAR to confirm their identity. The timeline begins once their ID has been verified. Parents have the right to access their child's personal data free of charge within 15 term days of the request. The personal data belongs to the child and not the child's parents. This is the case when the child is too young to understand the implications of subject access rights. For a parent to make a subject access request, the child must be able to understand their rights and the implications of a subject access request or have given their consent.
The Information Commissioner's Office (ICO), the organisation who upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of children accessing Springboard would be granted without the permission of the child.

Springboard will always ask for parental consents. These include consent such as taking photos for use in the setting and for publicity, the sharing of records with other professionals, administering medication, outings, first aid, face painting and applying sunscreen. These consents will all be asked at the point of registration of a child, (the starting process with Springboard) and usually annually therein. Parents will be given specific information regarding each of the consents and are asked to tick a box for each consent. This ensures that the process is clear and informed.
Written consents are obtained regularly whenever data is shared. This ensures that the consents are specific, and parents can make an informed choice and the decision is freely given. For example, a Team Around the Child (TAC) meeting, parents will be asked to consent to the meeting, agree the invitee list and consent to the agreed minutes being shared. Springboard must be able to demonstrate consent was given and to be able to show an effective audit trail.

Staff
Springboard processes data relating to those employed to work at Springboard. The purpose is to enable Springboard to operate and to:

- Enable individuals to be paid information is stored or shared with Sage, HMRC, Pension Auto-enrolment and NEST.

- Facilitate safe recruitment including but not limited to- DBS checks, references, Key-pad entry database (HikVision)

Staff personal data in stored online using Nursery in a Box (NIAB) a cloud based system and includes but is not limited to:
information such as:

- Contact details
- National Insurance numbers
- Salary Information
- Qualifications
- Date of Birth
- Next of kin
- Medical information

Personal data is retained as detailed in the data storage table within this document.

Trustees

Springboard processes data relating to those who volunteer as Trustees for Springboard. The purpose is to enable Springboard to operate and to:

- Facilitate safe recruitment including but not limited to- DBS checks, Ofsted suitability approval, references
- Completing annual returns for Companies House and the Charities Commission
- Compliance with fundraising platforms to prevent money laundering including but not limited to PayPal, Just Giving and Virgin Money Giving.

Trustee personal data in stored online using NIAB and includes but is not limited to:
information such as:

- Contact details
- National Insurance numbers
- Date of birth

Personal data is retained as detailed in the data storage table within this document.

Volunteers

Springboard processes data relating to those who volunteer at Springboard. The purpose is to enable Springboard to operate and to:

- Facilitate safe recruitment including but not limited to- DBS checks, references

Volunteer personal data in stored online using NIAB and includes but is not limited to:

- Contact details
- Medical information
- Date of birth
- Qualifications
- Next of kin

Personal data is retained as detailed in the data storage table within this document.

Visitors

During usual operating hours, all staff and visitors will be signed-in and out electronically, using

NIAB. Only staff can access the signing in screen, therefore visitors cannot see confidential information.
Outside of usual working hours or alternatively when activities are taking place off site, a paper signing in book/ sheet can be used which has GDPR compliant pages (no personal information is visible to anyone else using the signing in book).

Website
Springboard will collect and process the following categories of information /data about you:

- **Information you give us.** This is information about you that you give us by filling in the contact form on the website (**Site**), interacting with the Site or by corresponding with us by phone, e-mail or otherwise. The information you give us will include your name, address, e-mail address and phone number.

  If you are booking a workshop further personal information is required and this will include your email and any relevant accessibility information.

  If you are purchasing from the shop, you will be entering your name, address, email, and payment / card information into a third party called 'Stripe'. Full details of their security and privacy statement can be found on their website. https://stripe.com/gb/privacy#security-and-retention

- **Information we collect about you.** This is information that we collect automatically about your visit during your time on the site. It typically involves technical information and is often collected using small data files called "cookies". This information helps us to provide you with a good experience when you browse the Site and to indicate where the Site requires improvement.

  More information on how cookies work, what cookies we use and why can be found in our Cookie Policy (see separate policy).

Social Media platforms
We operate social media platforms. These platforms are, in most cases, operated outside of the EU and do not comply with current Data Privacy Act and GDPR provision although they may well conform to the U.S Privacy Shield protocol.
It is our process and protocol that any personally identifiable data gathered on these platforms is only in response to users interacting out of their own volition with our social media pages. The contact is deemed as a legitimate business enquiry. Any personal contact data is removed from the site once the enquiry is processed, or the user has requested so.

Analytics
Our website uses Google Analytics to collect information about how visitors use our website. We anonymise this data at the point of collection and automatically delete user and event data that is older than fourteen months.

Uses made of the information
All information about you that we collect or receive, whether of a personal or technical nature, may be used by us in the following ways:

- To carry out our obligations arising from any contracts entered between you and us and to provide you with the information, services that you request from us.
- To administer the Site and for internal operations, including troubleshooting, system and security updates, data analysis, testing, research, statistical and survey purposes.
- To improve the Site to ensure that content is presented in the most effective manner for you and for your computer.
- To allow you to participate in interactive features of our service when you choose to do so.
- As part of our efforts to keep the Site safe and secure.
- To comply with our record keeping and information storage obligations and policy (please see the "Where We Store Your Personal Data" section below for more details).

Disclosure of your information

We will only share anonymised information with:

- Analytics and search engine providers that assist us in the improvement and optimisation of the site.
- Third party support services, such as, but not limited to project management tools, accounting systems and hosting data centre.

We will disclose your personal information to third parties:

- If we are under a duty to disclose or share your personal data to comply with any legal obligation, or to enforce or apply our terms of use and other agreements; or
- To protect our rights, property, or safety, or those of our clients or others.

Where we store your personal data

Information that you provide to us will be stored on Microsoft Business OneDrive (365 Office) and Microsoft and Google forms. We will take reasonable steps to protect your information in accordance with this policy, including (without limitation):

- Installing a secure firewall.
- Using anti-virus protection software.
- Encrypting data; and
- Carrying out regular back-ups.

Information will also be stored on a secure Nursery software cloud-based system: Nursery in A Box (NIAB). Communication made using NIAB is secure and this is our preferred method of communication to parents, especially when sending documents.

All data sent via website forms is passed through a third-party relay service and deleted after 30 days.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of any data transmitted to our Site; and any such transmission is at your own risk. Once we have received

your information, we will use strict procedures and security features to try to prevent unauthorised access.

Our website and social media contain links to and from the websites for other agencies we work alongside. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Springboard use Microsoft Teams and Zoom for hosting virtual meetings/ workshops and calls. Springboard will create a meeting using these applications and send a link for participants to join the call. Both applications store some data and further information can be found below:

Zoom

Zoom stores basic information including, email address and password. Company name, phone number, and a profile picture are all optional to provide. Basic technical information, which would include the user's IP address and device details. If meetings are recorded this will be stored in the cloud and will be password protected. Further information can be found at https://zoom.us/privacy Zoom complies with all applicable privacy laws, rules, and regulations in the jurisdictions in which it operates, including the GDPR.

Microsoft Teams

Stores data including, your conversations using chats, shared files and if applicable any recordings.
Profile Data includes your e-mail address, profile picture, and phone number.
A detailed history of the phone calls you make, which allows you to go back and review your own call records.
This allows your administrators to diagnose issues related to poor call quality and service usage.
Information related to troubleshooting tickets or feedback submission to Microsoft.
Diagnostic data related to service usage.
Further information can be found at https://docs.microsoft.com/en-us/microsoftteams/teams-privacy

Docusign

Springboard have used Docusign to enable documents to be signed remotely and electronically, whilst providing a full audit trail.
Docusign collect personal data when a user registers, or logs into an account, reviews or signs an electronic document, contacts customer support or comments on-line.
Personal information includes name, email address, mailing address, phone number, or electronic signature, location, IP address, usage data, such as: web log data, number of clicks, domain names, pages and content viewed and the order of those pages, the amount of time spent on particular pages, the date and time you used our Services, the frequency of your use of our Services, error logs, and cookies.
Further details can be found at https://www.docusign.com/company/ privacy-policy

Survey Monkey

Survey Monkey is used by Springboard to collect and collate responses to surveys. Survey Monkey is a platform for hosting the survey and only collect the data we need to ensure the user experience. The data collected is protected, aggregated, and anonymised so you are not identifiable. Further details can be found at https://www.surveymonkey.co.uk/mp/legal/privacy/

General Data Protection Regulation (GDPR)

Springboard acknowledges GDPR came into effect in May 2018, expanding upon the previous DPA. GDPR harmonises the law between the European countries and expands legislation to incorporate all the technology advances since 1995.

GDPR still applies to the UK since leaving the EU, as the regulation applies to all European citizens wherever they live.

The GDPR gives individuals increased rights and these include

- The right to have their personal data deleted. An individual can request to have their data erased or deleted this applies to both hard copies and electronic documents held. Requests should be made directly in writing to either the manager or to the DPO. The Manager and the DPO would review all their data held at Springboard. As Springboard has a legal duty to maintain essential data not all data would be deleted, but Springboard would minimise what was held in accordance with the request.

- Data portability- individuals have a right to their data being transferred in an accessible form. This would be applicable when families move out of the area or transfer into another preschool or school. Springboard will always use standard formats e.g., PDF, Word, and Excel documents. Security will always remain a priority and documents would be password protected if sent electronically. The data would be sent to a mutually agreed destination e.g., email address or storage media destination.

- Right to have inaccuracies changed- a person has the right to the correct information being held about them. Errors or inaccuracies would be updated in a prompt timeframe, according to the usual working patterns of Springboard personnel. An annotation would be added to the records to state what correction has been made, when and by whom, to provide a full audit trail.

- Parents/ carers provide consent due to the age of the children attending Springboard. To verify the age of the children attending Springboard, birth certificates are requested and checked for verification.

- Stricter consents are required for text and email contact. Recipients of general emails will always be able to opt out and stop future contact. It should be clear that recipients have a choice to receive documentation.

Our **Data Retention Procedures** are as follows:

Secure storage and retention of all Data

Storage and access

Hard copies of personal data must be kept securely, in lockable, non-portable, storage containers with controlled access from authorised personnel.

Papers containing confidential and personal data should not be left on a printer, on a desk, in an office, on a notice board, where there is general access.

Where information needs to be taken off site (in paper or electronic form) staff must have this authorised by the manager and sign it in and out.
Trustees who store personal information on personal devices must follow the same security procedures.

'Personal' data is not held locally on any IT device, but stored centrally and protected by passwords, third party security firewalls and security software.
Due to the working practices, there may be some photographs temporarily stored locally on playroom tablets, which are password protected. Procedures must be followed to ensure the retention periods are followed to minimise the photographs held locally.
All staff are responsible for uploading and downloading data to ensure all data is stored securely. All devices are protected by passwords which are changed every six months, or when a member of staff leaves.

Access to electronic data is restricted to the relevancy of each member of staff and their individual role and responsibilities.
A back up of all electronic data is kept securely locked in the safe on site. Only the Manager and the DPO have access.

Handling
To protect the identity of the children, they are referred to by their initials. If more than one child has the same initials, the first two letters of their first name and the first two letters of their surname will be used to identify them. The Initials are used when sending out emails, meeting requests and general correspondence to multi-agency professionals to reduce the risk of the data being linked to a person.
When sending a document electronically, it is password protected and the password sent by a separate email.

Electronic documents are password protected before sending. The password is sent in a separate email; however, the password could be sent using alternative mediums e.g., phone, and text. If it is not possible to send an electronic document securely, a hard copy should be sent by post but only to a confirmed and known individual and to a known address.

Retention
Data is retained in accordance with the Data retention table below, this applies to both hard copies and electronic files kept. The archiving procedure must be followed, and a retention date clearly labelled.

Disposal
Once the retention period has elapsed, Springboard will ensure all data is destroyed by secure means, e.g., by shredding. Files for destruction will be identified by a destruction date. There will be an administration period required for physically destroying the files this could be several months due to term time only operations.

	Data Storage	
	Document	**Retention Period**

Child	Individual Files	Minimum 6 years from end of placement. Recommended until the child is 21
Child	Child Protection Files	24 years
Setting	Press Clipping	6 months
Setting	Newsletters	2 years
Setting	Team meeting minutes	Minimum 10 years
Setting	Management meeting minutes	Minimum 10 years Recommended permanently
Setting	Health and Safety documentation (risk assessments /accident records)	Minimum 7 Years RIGGOR related Minimum 40 years COSHH related minimum 40 years
Setting	Complaint reports	10 years
Setting	Registers	50 years
Setting	Building records	10 years
Setting	Records relating to accident or injury at work	Minimum 12 years
Setting	Office Accounts – this includes the name of people who have made donations.	Minimum 7 years
Setting	Old Insurance policies/certificates	40 years
Staff	Application Form	Duration of Employment
Staff	References received	1 year
Staff	Records relating to promotion, transfer, training, disciplinary matters	7 years from the end of employment
Staff	Annual Leave Records	2 years
Staff	Sickness Records	3 years
Staff	Unpaid leave/special leave records	3 years
Staff	Appraisal /assessment records	5 years
Staff	References given	5 years from end of employment
Staff	Payroll and tax information	6 years from end of employment
Staff	Summary of record of service, i.e., name, position held, dates of employment	7 years from the end of the employment
Staff	Individual supervision notes	7 years

If there are any concerns with regards to Springboard's handling of personal data then contact should be made to either Springboard's Data Protection Officer- Anne Farrell or the UK's regulatory body ICO (Information Commisioners Office) on 0303 123 1113

Data Breach

Data Breach- if a member of staff, volunteer or trustee sees or makes a data breach this must be highlighted to the Data Protection Officer (DPO) and the Manager immediately. The DPO and the Manager will investigate the breach, change procedures as appropriate to prevent future breaches and report to the ICO if applicable. Data breaches must be reported to the ICO within 72 hours if there is an individual is likely to suffer damage, for example identity theft or a confidentiality breach.

The ICO must be informed of the nature of the breach, the number of data subjects, the categories of data and the proposed mitigation.
A letter should be written to all the subjects whose data has been breached (a template is available on the ICO's website), an apology should be made and practical advice concerning the breach.
Possible breaches would be an email circulation list not hidden, so all recipients can see each other's email addresses, this would be a breach but not reportable. A confidential document concerning a child, not password protected and sent to the wrong person, would be a breach.
Failure to report a breach would result in a fine, in addition to a fine for the breach itself.

Secure Storage, Handling, Use, Retention & Disposal of Disclosures and Disclosure Information

General Principles
As an organisation using the Disclosure Barring Service (DBS) to help assess the suitability of applicants for positions of trust, Springboard Chippenham complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure Information.
Springboard complies fully with its obligations under the Data Protection Act 1998 and other relevant legislation pertaining to the safe handling, use, storage, retention, and disposal of Disclosure information for all its documents/ records and has a written policy on these matters, which is available to those who wish to see it on request.
Storage and access
Disclosure information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties. At Springboard this is Manager /Deputy and/or Business Administrator
Handling
In accordance with Section124 of the Police Act 1997, Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Disclosures or Disclosure information has been revealed and it is a **criminal offence** to pass this information to anyone who is not entitled to receive it.
Usage
Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.
Retention
Once a recruitment (or other relevant) decision has been made, we do not keep Disclosure information for any longer than is necessary. This is generally for a period of a year, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep Disclosure information for longer than a year, we will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.
Disposal
Once the retention period has elapsed, we will ensure that any Disclosure information is immediately destroyed by secure means, e.g., by shredding, pulping, or burning. While awaiting destruction, Disclosure information will not be kept in any insecure receptacle (e.g., waste bin or confidential waste sack). We will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure. However, notwithstanding the above, we may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the

position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

Privacy Impact Assessments

Privacy Impact Assessments (PIAs) demonstrate good working practice. The DPO and the Manager will use the assessment tool, a standardised template to analyse current processes to comply with the GDPR by identifying risk areas and reducing the risks. When new processes or technology is implemented it is paramount a PIA is completed at the implementation stage to minimise any possible risk of data breach. A PIA can demonstrate to the ICO, how Springboard complies with the DPA/GDPR and reduce the likelihood of Springboard failing to meet its legal duties. A log, listing all the PIAs completed will be maintained.

The PIA assessment template can be found using the link below-

https://ico.org.uk/media/1042836/pia-code-of-practice-editable-annexes.docx

Changes to our privacy policy

Any changes we make to our privacy policy in the future will be updated on our website www.springboardchippenham.co.uk.

Cross reference policies

Accident Reporting
Safeguarding Children
Equality and Diversity
Comment, Compliments and Complaints
SEN
Conflict of Interest
E-Safety
Disciplinary and Dismissal
Staff well-being
Admissions
Allegations Against Staff
Whistleblowing
Confidentiality
Working with Parents
Looked After Children
Staff Safety
Grievance
Competency and Capability

This policy was adopted at the Management Committee meeting of Springboard Chippenham

Held on Date to be reviewed:

Signed By:

Name of signatory: Chris Nunn Role of signatory: Chair