WELLSPRING SETTLEMENT
GDPR – Privacy and Information Sharing Policy

INTRODUCTION AIM AND SCOPE OF THE POLICY

Data Protection Principles

Everyone responsible for processing personal data (data processors) must follow strict rules called 'data protection principles'.

Data Processing in GDPR means the 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 of personal data.

The ICO describes personal data as information that relates to an identified or identifiable individual. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address.

Images **-** Images such as photographs and CCTV footage are also classed as personal data. See separate Internal Communications Guide and CCTV Procedure for guidance.

Everyone must make sure that personal data is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Individual rights under UK GDPR

Under the Data Protection legislation, data subjects have the following rights with regards to their personal information.
This applies to staff HR data as well as data collected for the organisation's charitable activities.

- the right to be informed about the collection and the use of their personal data
- the right to access personal data and supplementary information
- the right to have inaccurate personal data rectified, or completed if it is incomplete
- the right to erasure (to be forgotten) in certain circumstances
- the right to restrict processing in certain circumstances
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- the right to object to processing in certain circumstances
- rights in relation to automated decision making and profiling
- the right to withdraw consent at any time (where relevant)
- the right to complain to the Information Commissioner

Responsibilities/ Employees Duties

Wellspring Settlement has two Data Protection Officers (DPO's) Sally Jobling – HR Officer and Beth Wilson – CEO.

The DPOs determine the purpose, reason and type of personal data we collect from recruitment candidates and employee's personal information and sensitive data gathered from service users, contractors, volunteers or visitors, will be determined by the services offered.

Wellspring Settlement has a legal obligation to keep a record of processing activities (ROPA) which all staff will be required to maintain.

SharePoint/staff folder

Wellspring Settlement Data Protection Officers are responsible for.

- Ensuring HR records are compliant with UK GDPR legislation
- Reporting data breaches to the ICO where applicable
- Responding to the data subject following a Subject Access Request
- Maintaining the log of data breaches
- Ensuring staff are trained in line with this policy
- Ensuring that this policy reflects current legislation

All employees, contractors and volunteers as data processors are responsible for

- Ensuring data is processed in accordance with an individual's rights as listed above
- Ensuring all data is processed in accordance with the Data Protection Principles
- Ensuring any Subject Access Requests are passed to Sally Jobling – HR Officer (DPO) without delay

- Reporting any personal data breaches or potential breaches to Sally Jobling- HR Officer (DPO)
- Ensuring data subjects are given privacy information, as detailed in the Privacy Notice, as soon as personal data is collected.
  This must include, giving organisation name and contact details, the reason for processing data, who data will be shared with and why, how long it will be kept, the individuals rights regarding their data and how to request any action be taken with their data and how to lodge a complaint.
- Ensuring data is kept no longer than set out in the Retention Policy (Appendix A)
- Ensuring all data is processed lawfully.
- Ensuring data is as accurate as possible.

The lawful bases for processing are:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Data storage and security (see also IT Policy)

All employees, contractors and volunteers must ensure that all personal data is:

- Accessible only by those who need to use it
- Kept; in a secure environment - password protection if electronic (PC. Laptop or phone) or in locked storage devices within a secure environment if on paper (hard copy).
- Not disclosed either orally or in writing, whether accidently or otherwise, to any unauthorised employee, volunteer, service user, partner organisation or other third party.
- Only disclosed to a third party where consent in place beforehand or another lawful basis applies

DATA AND INFORMATION SHARING WITH PARTNER ORGANISATIONS

Whilst not directly a legal requirement, it is good practice to have in place a Data Sharing Agreement with any individual or organisation Wellspring Settlement shares data with. Such agreements may be a requirement of a funder or partner organisation.

An agreement protects the organisation in case of a data breach and goes toward compliance with the duty of accountability.

See Appendix 3 for Data Sharing Agreements. Service Managers have the responsibility for ensuring Data Sharing Agreements are in place with all partner organisations or funders and forwarded to Sally Jobling – HR Officer (DPO).

Employee Data

Wellspring Settlements HR will seek consent from employees to process their data.

Wellspring Settlement will only process personal information which is relevant to the employment relationship (potential, current or past)

Personal information processed by Wellspring Settlement may relate to:

- Contact details – name, address, email, telephone number.
- Recruitment and career development, including references and T&C's of employment.
- Pay and remuneration including payroll, tax, national insurance, pension and other benefits or deductions.
- Probation, Supervision and Appraisal and training records.
- Disciplinary and Grievance records (this is not an exhaustive list).
- Sensitive personal data processed and retained by WS may relate to; sickness (pay and leave), absence, obligations arising under the Disability Discrimination Act, Maternity, Paternity, Shared Parental leave, Pension Capability, Equal opportunities monitoring. (This is not an exhaustive list).
- Wellspring Settlement may further process and retain personal or sensitive data where it is required to do so under any statute.

All employees have a duty to check that any information that they provide to WS in connection with their employment is accurate and up to date, informing Wellspring Settlement of any changes or errors e.g. change of address cannot be held accountable for errors arising from changes about which it has not been informed.

Staff can access most of these records in their SharePoint staff folder and can request sight of any other records by making a Subject Access Request (see below).

SUBJECT ACCESS REQUESTS (SARS)

Individuals have the right to access and receive a copy of their personal data, and other supplementary information, known as a subject access request or 'SAR'.
Individuals can make SARs verbally or in writing, including via social media and to any member of the organisation. A third party can also make a SAR on behalf of another person, if they can prove they are entitled to act on behalf of the individual.

Wellspring Settlement will respond to a Subject Access Request without reasonable delay and usually within one month (30 days) of receipt of the request. This may be extended by 2 months if the request is complex or numerous. Sally Jobling - DPO must be notified of all SAR's.

The information will be supplied by way of an electronic copy, unless reasonable

adjustments are being taken into account, or the data subject agrees otherwise.

Wellspring Settlement shall provide access to the information unless doing so would infringe upon the rights of a third party or any legal exemptions applied. Information regarding third parties may be redacted.

SERVICE USER DATA

Personal information is gathered from Service Users/Clients only in so far as essential for the administration of the service offered. See Wellspring Settlements first contact form. Service Users/Clients are expected to complete a privacy notice/consent form as part of the first contact form, authorising us to retain their data. A more basic First contact form may be used in certain circumstances e.g. where it is not considered to be proportionate with the service provided to ask for the level of data on the full First contact form. In addition, Family Centre services may ask for a more detailed form to be completed, including details of children.

If we do not hold first contact forms/consent from Service Users/Clients, only data which does not identify them may be recorded e.g. number of people attending a specific activity.

Some funding arrangements may require us to retain data about people using the service. In these circumstances, we should first seek consent from the individual and only where this cannot reasonably be obtained may we rely on another lawful basis for retaining the data, other than consent. In these circumstances, a record should be entered into the Record of processing activities (ROPA) the individual service users should be informed that this is a condition for the them to receive the service. The minimum data needed to satisfy the needs of the funder should be recorded. Advice may be sought from a DPO if necessary.

WEBSITE SECURITY

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

How we use cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to tailor it to best suit user needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. This information is collected anonymously and only records information when you browse through our website. A

cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Links to other websites:

Our website does contain links to enable you to visit other websites of interest easily. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

PERSONAL DATA BREACHES

The GDPR requires Data Controllers to notify any personal data breach to the applicable regulator and in certain instances the Data Subject [potential service user/client/volunteer/employee].
If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact –Sally Jobling – DPO. You should preserve all evidence relating to the potential Personal Data Breach.

Breach of personal data reporting form is available from the SharePoint Staff folder or from Sally Jobling.

An investigation will be undertaken and Wellspring Settlement will notify Data Subjects or any applicable regulator where we are legally required to do so.

RETENTION OF DATA

Wellspring Settlement will hold the minimum personal data and sensitive data personal data necessary to enable it to perform its functions, and for the minimum length of time according to our retention policy (Appendix A).

The retention period will never be for longer than necessary and in line with current good practice and statutory requirements.

In such instances as Wellspring Settlement retains any data longer than the stated period for reference or analysis or for the improvement of services, this data will be in a completely anonymised format.

The erasure or destruction of information which is out of date will be conducted in such a way as to preserve the confidentiality of the information.

STAFF TRAINING

Staff will receive training as part of induction on the requirements of GDPR and their responsibilities. Wellspring Settlements staff training group will have responsibility for ongoing training needs of individuals.

DISCIPLINARY ACTION

Wellspring Settlement expects all its employees to comply fully with this policy and the principles of the Data Protection legislation.

Disciplinary action may be taken against any employee who breaches any of the instructions or procedures in this policy.

Wellspring Settlement is committed to the highest standards of confidentiality in relation to all its' employees, volunteers and service users. As such any breach of this procedure will be regarded as a serious matter and could lead to dismissal.

SHARING DATA INFORMATION

Sometimes, situations may arise where it would be appropriate to break confidentiality or share information. Circumstances which may be considered as appropriate are as follows:

- Where the information is not confidential in nature
- Where the person whom the duty is owed has given explicit consent
- Where there is an overriding public interest in disclosure
- Where it is considered by the worker in receipt of the information that an individual will be placed at risk of physical danger and withholding information could cause harm or injury to an individual.
- Where there is a legal obligation to disclose information:
- it is disclosed or considered that a criminal offence has been or will be committed
- information discussed relating to acts of terrorism
- disclosure of information relating to the -protection of children or vulnerable adults

In such circumstances, the staff member considering making a disclosure without consent, should seek the views of their line manager before doing so and inform the DPO as soon as possible so this may be entered into the data breach log.

General

The GDPR allows processing for specific purposes and Wellspring Settlement will comply with the law as defined by the Data Protection Act. The use of personal or sensitive information will be collected with the Data Subjects given consent, and used fairly, stored safely and not be disclosed to any other person unlawfully. The Act applies to all types of personal information, which is stored on computers or held in written copy. There are some circumstances where information can be shared without the Data Subject's consent and these must pass the following test of lawfulness:

Do you have a legal power to share information?

- For example, the Crime and Disorder Act 1998 section 115 provides legal power to share information to prevent crime.

Are you compliant with Article 8 of the Human Rights Act 1998?

- Information sharing may not interfere with rights under Article 8 (respect for private and family life) unless it is in accordance with the law and necessary in a democratic society in the public interest, public safety for the prevention of disorder or crime, the protection of health or the protection of rights and freedom of others.

Are you compliant with common law obligations of confidence?

- Common law requires that information may not be lawfully disclosed when given in certain circumstances of confidentiality. Disclosure of confidential information can be justified if:

  -The individual to whom the duty of confidentiality is owned has consented to the disclosure.

  -There is an overriding public interest in disclosure.

  -Disclosure may be required by a court order or other obligation.

  -If the individual who is owed confidentiality does not have the mental capacity and their best interests are described in the record of the safeguarding procedure (Vulnerable Adults Policy

APPENDIX A – INFORMATION RETENTION SCHEDULE

Record	**Retention**	**Statutory Authority**	**Reason**
Accident Book / records / reports	3 years from the date of the last entry (or if the accident involves a child/young adult, then until that person reaches the age of 21).	RIDDOR 1995 Limitation Act 1980	Statutory
Accounting records	6 years	Section 221 of the Companies Act 2006	
Income tax and NI returns, income tax records and correspondence with the Inland Revenue	3 years after the end of the financial year to which they relate.	The Income Tax Regulations 1996	
Medical records and details of biological tests under the control	40 years from the date of last entry	The Control of Lead at work Regulations 2002	

of lead at work			
Coronavirus Furlough records	6 years for furlough records including amounts claimed, claim period per employee, reference number and calculations. For flexible furlough - usual and actual hours worked.	See: former statutory guidance 'Claim for wages through the Coronavirus Job Retention Scheme'	
Medical records as specified by COSHH	40 years from the date of the last entry.	COSHH Regulations 2002.	
Medical records under the control of Asbestos at work regulations.	40 years from the date of the last entry.	The Control of Asbestos at Work Regulations 2012.	
Medical records under the Ionising Radiations Regulations	Until the person reaches 75 years of age, but in any event for at least 50 years.	The Ionising Radiations Regulations 1999.	
Records of tests and examinations of control systems and protective equipment under the COSHH Regulations	5 years from the date on which the tests were carried out.	The COSHH Regulations 2002	
Records relating to children and young adults	Until the child/young adult reaches the age of 21 years	Limitation Act 1980	
Retirement Benefits Schemes- records for notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place.	The Retirements Benefits Scheme Regulations 1995	
Statutory Maternity Pay records, calculations, certificates (MAT B1's) or other medical evidence	3 years after the end of the tax year in which the maternity period ends.	The Statutory Maternity Pay Regulations 1986 Maternity and Parental Leave Regulations 1999	
Wage/Salary	6 years	Taxes Management	

records		Act 1970	
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover.	National Minimum Wage Act 1998.	
Records relating to working time and leave	2 years from date on which they were made	The Working Time Regulations 1998.	
Flexible working requests	18 months following any appeal. This is because a further request cannot be made for 12 months following a request plus allowing for a 6 month tribunal limitation period on top.	CIPD recommendation only	
Subject Access requests	1 year following receipt of the request	Data Protection Act 2018	
Record	**Retention**	**Non Statutory**	
Actuarial valuation reports	permanently		
Application forms and interview notes (for unsuccessful candidates)	1 year.		
Assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently		
Banning records	5 years after the date that the ban is spent		
Board of trustees meeting minutes	Permanently	Company Policy	
Finance records	6 years	Companies Act 2006	

Contracts and tendering Expression of interest Ordinary contracts Contracts under seal Issuing and return of tender Tender evaluation Successful tenders Unsuccessful tenders The process of awarding a contract Successful funding applications Unsuccessful funding	– 2 years after contract let; or not proceeded with. –6years after contract has expired. –12 years after contract has expired – 1 year after start of contract. -Ordinary contracts – 6 years after contract has expired. Contracts under seal – 12 years after contract has expires. -Ordinary contracts – 6 years after contract has expired. Contracts under seal – 12 years after contract has expires. -1 year after start of contract -Ordinary contracts – 6 years after contract has expired. Contracts under seal – 12 years after contract has expires. -Ordinary contracts – 6 years after contract has expired. Contracts under seal – 12 years after contract has expires.		

applications Funding contracts and service level agreements	-1 year after notification of refusal. -6 years after terms of the contract have expired.		
CCTV Images	6 months after the outcome of any formal decision or appeal	ICO retention practice	
Covid 19 vaccination records	This is 'special category' data requiring extra protection. Under the DPA employers can only keep this data for a good reason and if there is a lawful basis for processing it such as employee or public health duties.	Uncertain - employers should review whether they have grounds for the processing vaccination data. . As the pandemic retreats the justification for keeping data may change.	
Disciplinary and Grievance records	1 year after 'spent' time, dismissal -6 years after employment ceases.		
Inland Revenue approvals	Permanently		
Money purchase details	6 years after transfer or value taken		
Parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance.		
Pension records	12 years from the ending of any benefit payable under the policy		
Personnel files and training records (including disciplinary records	6 years after the employment ceases		

and working time records, appraisal)			
Redundancy details, calculations and payments, refunds, notification to the Secretary of State	6 years from the date of redundancy.		
References	Outgoing -up to 1 year, employers may be able to justify a longer retention period of six years, if they are concerned about defending any future claims. Incoming unsuccessful applicants – 9-12 months	CIPD Recommendation only	To meet the limitation period for potential defamation claims. Time limit for discrimination is six months plus possible time limit extensions.
Right to Work in the UK documents	2 years	Home Office recommended practice	
First Aid training	6 years after employment	Health and Safety (First Aid) Regulations 1981.	
Fire Warden Training	6 years after employment	Fire Precautions (Workplace) Regulations 1997	
Health and Safety representatives and employees' training	5 years after employment	Health and Safety (Consultation) Regulations 1996; Health and Safety Information for Employees Regulations 1989	
Records relating to staff working with children	25 years from termination		
MSK clients	8 years from date of last	Best practice retention of	

	contact	health records from the Chartered Society of Physiotherapists	
Community groups / class attendees	6 years from date of last contact	Section 5 Limitation Act 1980	
Senior Executives' records (that is those on a senior management team or their equivalents)	Permanently for historical reasons		
Staff supervision and annual appraisal notes.	3 years from date of appraisal.		
Service users including parents personal files and data	6 years after last attended date.		
Trade union agreements	10 years after ceasing to be effective		
Whistleblowing documents	6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately.	Public Interest Disclosure Act 1998 and recommended IAPP practice	
Trust deeds and rules	Permanently		
Volunteer records including recruitment and supervision			
Child protection records	10 years from last contact	This information is retained for this period in line with OFSTED and BAND recommendations. This is for the purpose of	

		evidence of any (but not limited to) child protection health or queries about procedural issues that may arise later in the child's life	
Adult education budget funding agreement records	14 years from the end of the financial year in which the last payment is made	Invoices, learner records and all other documents necessary to verify the provision of the contract	
Trustee records	5 years from the date of resignation or retirement.	Charity Commission	

APPENDIX B – PRIVACY NOTICE

Wellspring Settlement is committed to protecting your personal data and handling it responsibly.

This policy covers the personal data that Wellspring Settlement collects whenever you interact with us, including and not exclusive to, when you use our website and social media sites, use our services, community space, café, events, room hire and when you correspond with us such as email or over the phone. It also covers personal data that we may receive from a third party.

The sections below explain in more detail:

- The types of personal data we collect from you
- The types of personal data we receive from third parties
- Why we process your personal data.
- Who we share your personal data with
- Personal data transfers outside the EEA
- How long we retain your personal information
- Your rights to withdraw your consent and to object
- Your personal data rights
- How to contact us and exercise your rights.

Personal Data Wellspring Settlement collects from you

This policy covers personal data Wellspring Settlement collects whenever you interact with us, including when you use our services and facilities such as:

- Family Hub Services
- Social Prescribing/ Hospital Link Services

- BOOST Finance
- Food Club
- Arts /Physical Activities
- Community Engagement
- WS courses/ Groups/ Adult Education
- Events/Room Hire
- When using our website or social media
- Correspond with us, via email or over the phone

The personal data we collect form you may include:

- Name and contact details, race, ethnicity, religion, age, gender, identity, sexual orientation, employment status, disabilities you provide when you first attend a Service/Activity/Group/Volunteer/Work placements/Events/sign up to receive our newsletter via web forms (we may also collect IP addresses via our web analytics system (Google Analytics) or access the facilities including the Café/Community Space or Room Hire.
- Details of your children such as name, age, gender, disabilities
- Your payment and address details
- Marketing preferences and data consents
- Information about your attendance at Services/Activities/Groups/Courses/Events and other one-off activities arranged by Wellspring Settlement. Photos and video footage of you may be taken at events

Personal data Wellspring Settlement receives from third parties

- Referral agencies (eg, JotForm's, Google docs, local authority, GP's other partner organisations) for Service delivery including Social Prescribing, Boost, Hospital discharge, MSK Clinic.
- Referral agencies (Family Hub and Local authority) for children and family services.

Why Wellspring Settlement processes your personal data

This section explains the reasons why we process your personal data and our legal bases for doing so.

Consent-

If you have opted-in to receive information relating to Wellspring Settlement, then we will provide this information to you by email, text or phone. Wherever we rely on your consent to process personal data, you have the right to withdraw that consent.

Legitimate interests-

We process your personal data when necessary to pursue our legitimate interests in the following:

- To gather information about the people who use the Settlement.
- To identify gaps and evidence the need for other services,
- To access the right services and personal support.
- To promote events, special offers or other formation we think you may find interesting, such as our newsletter.
- To monitor progress and evidence for our Funders
- Monitoring, improving and protecting our services.

- Responding to comments or complaints
- Undertaking or inviting you to take part in market research
- Using incident reports and CCTV footage to protect the security of our staff and Users to help detect and prevent unlawful activity.
- Preventing, investigating and/or reporting fraud, terrorism, misrepresentation, security incidents or crime.

You have the right to object to any processing that we undertake for our legitimate interests.

Contract-

We process your personal data when we are administering your involvement in Services and Activities. eg. Children and Youth Services, Health and Social Care and Groups.

Legal Obligation-

We are legally required to process your personal data in cases where we need to:

- Obtain parental consent to provide services directly to children and young people.
- Respond to certain requests by government or local authorises.

Who Wellspring Settlement shares personal data with-

- Third party organisations which you have given consent to.
- Organisations whom you have an existing relationship with (e.g. organisations that have referred you to us).
- if there is a risk of serious harm or threat to life. This includes child protection concerns, suspicion of abuse or neglect of a vulnerable adult
- Police or other agents of the state where we are required to do so by law.

Personal data transfers outside of the EEA-

No data is transferred outside the European Economic Area.

How Long will Wellspring Settlement retain personal data-

Wellspring Settlement will hold the minimum personal data and sensitive data personal data necessary to enable it to perform its functions, and for the minimum length of time according to our retention policy (Appendix A). Wellspring Settlement will not sell, distribute or lease your personal information to third parties unless we have your consent or are required by law.

Your rights to withdraw erase, correct, or object-

Whenever we rely on your consent to process personal data, you always have the right to eraser your consent or correct your personal data. You also have the right to object, to any use of your personal data, as well as to processing that we undertake based on our legitimate interests.

How to contact us and exercise your rights-

Wellspring Settlement will do our best to assist with a query you have about your personal data. You can contact Sally Jobling our Data Protection Officer at any time using the contact details below. When you do so please provide your full name, preferred contact

information and a summary of your query.

Sally Jobling – Data Protection Officer
43 Ducie Road
Bristol
BS5 0AX
Sally.jobling@wsb.org.uk

If you have unresolved concerns, you also have the right to contact the Information Commissioner's Office

APPENDIX C - PROCEDURES BY SERVICE

Information Sharing Protocols

Records of processing and lawful basis | ICO

Family Hub

Wellspring Settlements family centre staff collect personal data and information using the children's centre membership form on behalf of Bristol City Council. This information is held and managed securely by Bristol City Council and also transferred into the Wellspring Settlements Focus electronic management system. The membership forms and registers of attendance are transferred from Wellspring Settlement to St. Pauls Children's centre using a nominated person collection service. The information is then input into the Bristol city council Estart electronic management system by the qualified Estart co-ordinator based in St. Pauls Children's centre. All family centre staff work to five information sharing protocols which are available to you on request:

- New births / Movers in and deceased under fives (Health)
- Under 5s known to social care
- Children attending other settings (Lead Teacher recording)
- Big Reach List – GP registration data
- Eligible 2 YOs (DWP)

Family Centre staff also work within the guidelines of the Bristol City Council privacy notice which is on view in the Family Centre playroom. The most recent version of the Privacy Notice will be available on the Bristol City Council website. www.bristol.gov.uk.

As part of the Ofsted registration requirements the family centre staff also work within the statutory framework for Early Years, information sharing and guidelines Information and Records see section 3 page 31. www.bristol.gov.uk.

Page **1** of **5**

INFORMATION SHARING WITH CHILDREN'S CENTRES
Children under 5 years known to Social Care

1. Background

The most recent Ofsted framework and national guidance for Children's Centres states that Centres will be expected to be aware of the numbers of children in need (CIN), looked after children (LAC or CLA) and children with child protection plans (CP) living in their reach area, and to offer services to children and families within these groups.
In order to support Children's Centres with meeting these requirements, certain information about these children will be shared with Children's Centres on a regular basis. This information should enable Children's Centres to have an accurate record of the numbers of children in these groups, and to track whether they are currently working with each of these families. In cases where they are not, this information will support Children's Centres in making contact, where appropriate, via case workers and their teams. This document is intended to support the information sharing process.
The Council has the power to share this information under the Local Government Act 2000, as sharing this information will help to promote the social well-being of families in the Bristol area, and will help to meet the Corporate Plan objective of "focussing on pre-natal and early years care and support for those families most in need, to give every child in Bristol the very best start in life possible".

2. Information that will be shared

The following information on children aged under 5 known to Social Care, including unborn children, will be shared with Children's Centres:

- Child's name, date of birth, age, gender and ethnicity
- Current type of involvement (CIN, CLA, CP) with the date of the initial referral to social care and social care involvement in previous quarter
- Indication of whether children have newly entered the system, changed type of involvement, left the system completely, or remained unchanged since data was last circulated
- Child's case worker, team and team contact number

Children's Centres will be supplied only with information about children under 5 living in their reach area who have social care involvement. This information will be taken from the Liquid Logic database for children's services, and represent a 'snapshot' at the end of the preceding quarter (e.g. the information issued in October will be as at 30th September).

Reach area will be determined from the child's current residential postcode. For CLA, this will be their current placement; for all other children this will be their primary address. It should be noted that some CLA with a restricted address will show City Hall as their place of residence; this may inflate the associated CLA numbers that relate to the pertaining reach area.

Data will indicate changes since the previous quarter end. It will be grouped as follows:

- Children who have started social care involvement
- Children who have changed level or type of involvement
- Children with social care involvement who remain unchanged
- Children who have ceased social care involvement.

Within each group, children will be sorted by type of involvement, and within this by social care team working with them. Any changes will be highlighted.

Centres will **not** be supplied with parent/carer names, contact details or addresses; this is to ensure that contact with parents/carers and children are made only after discussion with the relevant case worker.

Address information will not be supplied, because some addresses are restricted/confidential, and to avoid the risk of inappropriate contact being made. Contact details for the family can be made available by case workers where it is agreed this is right to do.

The information shared will relate to the Bristol social care database only. Information regarding children placed into Bristol by other local authorities is incomplete.

3. Timescales

Information will be collated and circulated by the Information & Analysis Team, Bristol City Council on a quarterly basis.
The information will be a 'snapshot' taken at the end of each quarter, with information taken from Liquid Logic as follows:

Date information collected Date information sent
30th September By 25th October
31st December By 25th January
31st March By 25th April
30th June By 25th July

The information will be sent to Children's Centres by the end of October, January, April and July.

4. Means of transmission

The data will be emailed securely by the Information & Analysis Team, in line with current corporate policy, in MS Excel format to nominated Children's Centre staff. The Information & Analysis Team will maintain a list of recipients for this information. Children's Centres should promptly inform the team of any changes.

5. Using the data

Data is primarily supplied to support identification of children with additional needs and their families. This data will, in particular, be useful in identifying numbers of children falling into one of the three social care categories referred to as part of providing evidence to Ofsted of take-up of services within these groups.
Children's Centres may want to make contact with families, including non-parental carers, and parents whose children are not currently living with them, in order to provide support or encourage them to access services. Any Centre wishing to do so, should first contact the child's case worker or team, in order to check that there are no safety concerns around making contact, and discuss the suitability of offering services. Where appropriate, case workers will be able to supply carer/parent names and contact details, or pass on messages.

In some cases, Children's Centres will already have contact with children or families who have social care involvement, though Centres may not be aware of this prior to receiving the data. Centres are strongly encouraged to contact the child's case worker or team before making further contact with the family, in order to ensure there are no areas of concern or confidentiality of which the Centre is not aware.

All data received must be stored securely and only for the purposes for which it is intended. It should be stored so that only those who should have access can gain access, and it is preferable that there is an auditable trail for access. This means for electronic data a separate drive, and should always be password protected. The Data Protection Act states that you should only keep data for as long as is considered necessary for the purpose for which it was first collected, and that personal data should be accurate and up to date. The recommendation is that all data, whether electronic or paper-based, is stored for at least one year.
The information is not to be used for any other purpose as advised in section 4.8 of Schedule 4 relating to Part One of the Children's Centre Service Agreement.

6. Sharing information within and outside the Centre

The information provided by the Information & Analysis Team should be held confidentially and not shared except in the specific circumstances given below.

6a. When information may be shared

Information provided in this dataset should only be shared within Centres, and then only on a 'need to know' basis. It is recommended that information on a particular family only be shared with that family's or child's worker.

This information may be shared with a single admin worker (for example, to run checks on eStart). In all cases of sharing this data, staff should be given a copy of this protocol, and reminded of the need for confidentiality, whether with other professionals outside the Centre, with staff within the Centre, or with families and visitors to the Centre.

Information should be shared within the Centre if it is required to enable the Centre to provide their assessment for the child protection plan or care plan; and if it is

required to enable the Centre to provide the right help and support for the child and their family.

Families included in this information should have been made aware by their case workers that their information will be shared to facilitate support for them. Nonetheless, Centres should continue to exercise care and caution when approaching any family members, carers or children to offer support or services.

6b. When information should NOT be shared

Information provided in this data set should not be shared with the following:

- NHS and health partners
- Other sites used by the Centre for service provision
- Non Bristol City Council services being provided through the Centre (other than a service provided by a voluntary early years setting that has been commissioned by the Children's Centre to provide part of the Children's
- Centre core offer with a written Service Agreement in place)
- Any other agency that Centres may be working with
- Any other Bristol City Council service e.g. Housing, Schools etc
- Anyone making a general enquiry about a child or family

If there is any doubt about whether information can be shared with a particular party, please refer to the contact details below.

This protocol applies only to information provided within the dataset. Any other information sharing (for example, other agency involvement shared with Social Care or Health) should be covered by the Children's Centre's own confidentiality/ data protection/ information sharing/ safeguarding policies.

All information is provided in accordance with Bristol City Council's Data Protection policy http://www.bristol.gov.uk/page/data-protection-act.

7. eStart

8.

All data, including the child's current level of social care involvement, should be treated with discretion, particularly when the family is not accessing the Centre, or has not chosen to disclose social care involvement. Recording of this data on eStart and other similar databases should be done with care around potential Data Subject Access requests (for example, an abusive partner asking for information about their record should not be able to access records that give the child's or ex-partner's current address).

Any Children's Centres receiving notification that a child has ceased social care involvement should ensure that any flags on eStart regarding this are removed, and that the child's record is updated to show social care involvement has ceased. Information regarding any social care involvement is collected on the Children's Centre membership form. For families living within the Centre's reach area, it is recommended that this information is reconciled with the data shared quarterly under the terms of this protocol.

9. Limitations of the data

Children move in and out of social care involvement and their social care status can change over short periods of time so the information may have become inaccurate between the time of recording on the social care database and the time of receipt by Children's Centres.

The file will not include the following:

- Children who have had a social care referral that has opened and closed within the same quarterly reporting period.
- Children who have moved address to another Children's Centre reach area or Local Authority.
- Information on a child that has been entered onto the social care database after the time the quarterly report has been run (late recording). This means that on occasions children you expect to see will be missing from the list, and children you do not have a record of are on the list as existing or closing cases.

Late recording on the social care database can occur due to the complexities of social care procedures and is more likely to occur for LAC and CIN cases. If you notice any discrepancies between the information provided and the information held at your setting, please contact Kam Govind for clarification.

10. Contacts

Early Years Team:
Rachel Williams, Early Years Partnerships & Information Manager (0117 37 73237)
rachel.williams@bristol.gov.uk
Information & Analysis Team:
Kam Govind, Information & Performance Officer (0117 90 37399)
kam.govind@bristol.gov.uk
Date: January 2016
To be reviewed: March 2017
\\ds\data\PPP\IAS\Data\Info Sharing with CCs\Social Care\Protocol for social care info sharing with CCs v2.docx