Partnership Personal Information Sharing Agreement (PISA)

April 2019

CONTENTS

1. Introduction

1.1 This Personal Information Sharing Agreement (PISA) covers the work of the Bournemouth, Christchurch and Poole Safeguarding Adults Board, Bournemouth and Poole Safeguarding Children Board and the BCP Community Safety Partnership (hereafter referred to as the Partnerships).

1.2 The PISA exists to facilitate the exchange of personal information to meet the aims of the individual Partnerships (Appendix 1) and more specifically to comply with the requirements of Section 9 of the Domestic Violence, Crime and Victims Act 2004 to establish and coordinate a **Domestic Homicide Review**, Section 44 of the Care Act 2014 to conduct a **Safeguarding Adults Review** and the Children Act 2004 as amended by Children and Social Work Act 2017 and The Child Safeguarding Practice Review and Relevant Agency (England) Regulations 2018 to **conduct a Child Safeguarding Practice Review** (hereafter referred to as Reviews).

1.3 The PISA is made under the Dorset Information Sharing Charter (DISC) and the agencies listed in Appendix 2 have signed up to the agreement.

1.4 The PISA will also be applicable to other organisations as necessary to meet the aims of the Partnerships and the purpose of the Reviews. If additional organisations are required to share and receive personal data they will be required to sign up to the PISA.

2 Lawful Basis for the Sharing of Personal Information

2.1 Any decision to disclose or share information should adhere to the six Data Protection principles.

- Processing must be lawful and fair;
- Purposes of processing must be specified, explicit and legitimate;
- Personal data must be adequate, relevant and not excessive;
- Personal data must be accurate and kept up to date;
- Personal data should be kept for no longer than necessary;
- Personal data must be processed in a secure manner.

2.2 Article 9 of the General Data Protection Regulations (GDPR) requires that the processing of 'special category' or sensitive personal data must have a lawful basis. For the purposes of reviews that lawful basis is Article 6 (e) of the GDPR which states 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.'

2.3 The following legislation provides the statutory powers for the partner organisations to share special category (sensitive) personal data under this PISA:

- General Data Protection Regulations (2016)
- The Law Enforcement Directive (2018)
- The Data Protection Act (2018)
- The Human Rights Act (1998)
- The Crime & Disorder Act (1998)
- The Domestic Violence Crime & Victims Act (2004)

- The Children Act (1989 and 2004)
- The Care Act (2014)
- The Common Law Duty of Confidentiality

2.4 Under part 3 of the Data Protection Act 2018, states, Dorset Police as detailed under Schedule 7 of the Act are identified as a 'competent authority' meaning it has a statutory function process personal data for any of the law enforcement purposes – prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Any processing carried out by a 'competent authority' which is not for the **primary purpose** of law enforcement will be covered by the GDPR and Part 2, Chapter 2 of the Act.

3 General Process for Requesting Sharing and Processing Personal Information

3.1 There are circumstances when each of the Partnerships and associated groups conduct a piece of work which requires access to personal data, for example multi-agency safeguarding audits, specific pieces of quality assurance work or work to gain a greater understanding of the dynamics of a specific crime and disorder issue and/or safeguarding issue.

3.2 When needed, personal data will be requested from agencies, in writing using a standard letter or documented in the minutes of a meeting they attended. The agencies the Partnership requests information from will be known as 'the data controller.'

Data Controller

3.3 The data controller will have all of the legal obligations given to them by the Data Protection Act 2018. Following the written request for personal information the data controller will:

- need to collect the personal data and establish the legal basis for doing so;
- determine which items of personal data to collect, the purpose or purposes the data are to be used for;
- whether to disclose the data to the requestor;
- whether subject access and other individuals' rights apply i.e. the application of exemptions;
- how long to retain the data or whether to make non-routine amendments to the data;
- Personal data is shared in line with each organisations Privacy Notice. Each organisation's link to their individual Privacy Notices can be found in Appendix 1 Signatures;
- Under the GDPR and Data Protection Act 2018 information can be shared without consent if, there is a lawful basis to do so, such as where safety may be at risk, based on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

3.4 The data controller is the service/department of the organisation that supplied the sensitive personal data to complete a specific piece of work. As owner of the personal data, the data controller will have overall control of the data processing operation and must make the decisions listed in paragraph 3.3 after receiving a request from the Partnership. This determines the purposes for which and the way any personal data is to be used. The data controller will not unreasonably refuse a valid, lawful request for data.

Data Processor

3.5 The data processors will have the legal obligations given to them by the Data Protection Act 2018 and are those requesting, receiving, holding, disseminating and using the information in line with the agreement with data controller. The data processor/s will be identified prior to the information being requested. This could be an individual organisation or a group of individuals from a range of agencies. For example, in the case of an audit it would be the panel established to oversee the audit.

3.6 The length of time personal information will be retained by the data processor will be set by the data controller.

General Rules

3.7 Hand written notes detailing personal information should be kept to a minimum and be taken only for the purposes of agencies noting their actions. Typed minutes will be the formal record of what was discussed at meetings and these will be securely stored electronically. If hand written notes need to be retained they should be scanned and either password protected or stored in a secure file. The original paper version destroyed.

3.8 All documentation containing personal data relating to victims, perpetrators, wider friends and family should be marked 'OFFICIAL SENSITIVE' and should only be transmitted by secure E mail.

3.9 All data provided and shared by the Partnership should be stored and processed so that its integrity and confidentiality are maintained always. All partner agencies involved should store and process personal data in line with both this PISA and their local policies and protocols.

3.10 Any information held electronically should be password protected or stored in a secure area which cannot be accessed by staff not involved in the activity.

4 Lawful Basis for Sharing and Processing Personal Information in relation to Reviews

4.1 Statutory guidance has been produced outlining how each of the reviews should be conducted.[1]

[1] Safeguarding Adults Reviews - Paragraph 14.162 of the Care Act Statutory Guidance 2018
Domestic Homicide Reviews Statutory Guidance 2016
Child Safeguarding Practice Reviews - Chapter 4 Working Together 2018

4.2 To achieve the purpose of all Reviews there is always a need to access sensitive personal data regarding the victim and other people of interest e.g. perpetrator or wider family members etc. The lawful basis for this access is detailed in paragraph 2.2 and 2.3.

4.3 Personal information will be routinely requested from:

- BCP Council
- Dorset, Devon and Cornwall Community Rehabilitation Company
- Dorset Clinical Commissioning Group
- Dorset Healthcare University Foundation Trust
- Dorset Police
- Dorset Youth Offending Service (For Children Safeguarding Practice Reviews)
- National Probation Service

4.4 The type of information requested will include health records including mental health, housing records, education records, interaction with the police and/or services provided to them by Adult, Probation and Children Services. Personal information may also be requested from other statutory and voluntary sector agencies as required.

Initial Scoping and Individual Management Reviews

4.5 The Review Panel will determine the scope of the Review to fulfil the purpose outlined in the statutory guidance. The Panel usually consists of those organisations listed in Paragraph 4.3.

4.6 The Chair of the Panel will approve any new agencies to join the Panel and retains the right to reject such applications if they are deemed unsuitable or inappropriate or if the agency is unwilling to sign up to this PISA.

4.7 Following the scoping exercise the Review Panel determines what personal information to request regarding which individuals and over what timescale.

4.8 As identified in paragraph 4.3 and 4.4 there are a wide range of agencies, hereafter referred to as data controllers, who hold relevant personal information regarding the individuals identified within the scoping exercise.

4.9 Information will be requested from these agencies in writing using a standard letter or documented in the minutes of a meeting they attended.

4.10 Following the request from the Review Panel the data controller will fulfil the obligations under paragraph 3.3 and 3.4.

4.11 The data processors for a Review are the members of the individual organisations that make up the Panel and the Chair and Independent Overview Author. The Chair and Independent Overview Author will be contractually required to comply with the requirements of the Data Protection Act 2018 and associated legislation.

4.12 Within the terms of the agreement with the data controller, the data processor may consider all actions listed in paragraph 3.5.

Overview Report, Executive Summary, Synopsis of Learning and Action Plan

4.13 The Independent Overview Author drafts the Overview Report for all the Reviews and also an Executive summary in the case of a DHR. These reports bring together all the information gathered as part of the review and draws overall conclusions from this information. Within the draft reports all personal information is anonymised.

4.14 The reports are marked OFFICAL SENSITIVE and this marker is maintained until the date of publication.

4.15 Each data controller is responsible for ensuring the information they submitted is accurately, fully and fairly represented in the draft reports.

4.16 An anonymised restricted version of the report and associated action plan will be produced and provided to the lead Partnership for sign off.

Publication of the report

4.17 An anonymised version of the final Overview Report and Executive Summary (DHR only) are published in accordance with the statutory guidance.

5 Retention Rules for Reviews

5.1 The data controller will dictate how long personal data can be retained by the data processor.

5.2 An audit trail will be retained of any discussion or decisions made by the lead Partnership and/or Review Panel by the lead organisation identified within the panel. These will be kept for six years following sign off by the relevant Partnership.

6 Data Breaches

6.1 A data breach is defined as an incident that leads to the loss, theft or inappropriate disclosure of personal information or the exposure of personal information to such risks, whether they take place or not. In certain circumstances it can also include the unauthorised alteration or destruction of personal information.

6.2 If a data breach occurs the individual should follow their organisational policy regarding this issue and if they are not the data controller they should notify the data controller that their information could have potentially been compromised

7 Subject Access

7.1 If an agency receives a subject access application and personal data is identified as belonging to another agency, it will be the responsibility of

the receiving agency to contact the data controller as the owners of the information to determine if they can or cannot comply with the request.

8 Review of the Partnership PISA

8.1 The Partnership PISA will be three yearly or as the need arises. The agreement made herein however, remains in force irrespective of whether the agreements officially reviewed.

Review Date March 2022

APPENDIX 1

BCP Community Safety Partnership
The BCP Community Safety Partnership (CSP) aims to reduce crime and the fear of crime, address risk, threat and harm to victims and local communities; and facilitate the strengthening of BCP's communities in the delivery of local initiatives.

Bournemouth, Christchurch and Poole Safeguarding Adults Board
The Bournemouth, Christchurch and Poole Safeguarding Adults Board is a statutory multi-agency partnership which exists to ensure that effective arrangements are in place across the county to support and safeguard adults who have care and support needs and are at risk of abuse and neglect.

Bournemouth and Poole Safeguarding Children Board
The objective of the BPLSCB is to coordinate and ensure the effectiveness of what is done by each agency on the Board for the purposes of safeguarding and promoting the welfare of children in BCP.

APPENDIX 2

Signatories to the PISA:

Signed by ……..

For and on behalf of BCP COUNCIL

Printed Name:……

Designation:……

Dated……..

Signed by……

For and on behalf of DORSET POLICE

Printed name:……..

Designation:……

Dated:……..

Privacy Notice: https://www.DORSET.police.uk/news-information/legal-privacy/

Signed by……

For and on behalf of NHS DORSET CLINICAL COMMISSIONING GROUP

Printed name:…….

Designation:……

Dated:……..

Signed by……

For and on behalf of THE DORSET, DEVON AND CORNWALL COMMUNITY REHABILITATION COMPANY LIMITED

Printed name:…….

Designation:……

Dated:……..

Signed by……

For and on behalf of THE NATIONAL PROBATION SERVICE

Printed name:…….

Designation:……

Dated:……..

Signed by……

For and on behalf of DORSET HEALTHCARE UNIVERISTY FOUNDATION TRUST

Printed name:…….

Designation:……

Dated:……..

For and on behalf of DORSET AND WILTSHIRE FIRE AND RESCUE SERVICES

Printed name:…….

Designation:……

Dated:……..

Signed by……

For and on behalf of DORSET YOUTH OFFENDING SERVICE

Printed name:……..

Designation:……

Dated:……..

Signed by……

For and on behalf of POOLE HOSPITAL NHS FOUNDATION TRUST

Printed name:……..

Designation:……

Dated:……..

Signed by……

For and on behalf of ROYAL BOURNEMOUTH AND CHRISTCHURCH HOSPITALS NHS FOUNDATION TRUST

Printed name:……..

Designation:……

Dated:……..

For and on behalf of SOUTH WEST AMBULANCE SERVICE FOUNDATION TRUST

Printed name:……..

Designation:……

Dated:……..

APPENDIX 3

TAKEN FROM SECTION 9 OF THE DISC – DATA BREACH MANAGEMENT
(with additional clause at 6.4 requested by Dorset Police)

Purpose

1.1 All organisations that process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. It is the individual responsibility of all who use, keep or collect personal data to apply the provisions of the Data Protection Act 2018 and GDPR.

1.2 All partner organisations signed up to the DiSC must take steps to ensure that shared personal data is always kept secure against unauthorised or unlawful loss or disclosure.

1.3 This guidance sets out the areas that should be considered by staff and managers in the event of a data or information security breach.

Definitions

2.1 A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual who is unauthorised to do so.

2.2 Data breaches may involve personal health data, personal identifiable data, trade secrets or intellectual property.

2.3 A data security breach can occur when (this list is not exhaustive):

- hard copy files or records are left unattended, lost or stolen;
- laptops, ipads, phones, data sticks or any other removable portable device holding personal or sensitive data are lost or stolen;
- databases or case file management systems are accessed by unauthorised users – either accidentally due to inadequate system access controls or intentionally by hackers;
- equipment fails;
- sensitive data is posted, faxed or emailed to the wrong recipient;
- inappropriate data is released as part of a Subject Access Request;

- unforeseen circumstances such as a fire or flood damage storage or buildings;
- data is obtained by deceiving the person who holds it – blagging offences;
- data is obtained by eavesdropping to phone calls, viewing pc screens in unprotected public spaces - shoulder surfing.

Data breach investigation

3.1 Organisations should have an agreed process for responding to and investigating suspected or actual data breaches which will involve the Information Governance (IG) lead.

3.2 Where data is shared between organisations, the Personal Information Sharing Agreement (PISA) should state which organisation will lead the investigation in the event of the loss of shared data.

3.3 Each incident of data loss will require a subtly different response plan however, there are four important elements to any breach management plan:

- containment and recovery;
- data sensitivity risk assessment;
- notification/reporting of breach;
- response, evaluation and review.

Containment and recovery

4.1 The investigator should establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. In all cases, the affected organisation's information governance leads should be informed. They will take responsibility for:

- notifying key people within their own organisations, which might include the SIRO, legal teams, ICT security leads, communications team;
- liaison with the Information Commissioner's Office (ICO) and the data subject/s where appropriate.

4.2 The investigator should establish whether anything can be done to recover any losses and to limit the damage caused by the breach. In all cases, attempts should be made to recover the data - it is not acceptable to rely on someone who has inadvertently received or found the information to destroy or return it.

4.3 It may be appropriate to consider informing the police depending upon the nature of the information that has been lost.

Data sensitivity risk assessment

5.1 To understand the impact of a data breach, the extent of potential damage, and to agree an appropriate course of action, it is helpful to undertake a data sensitivity risk assessment.

5.2 The assessment should consider the following:

- what type of data is involved?
- how sensitive is it? Some information is sensitive because of its very personal nature (health records) whilst other information is sensitive because of what might happen if it is misused (bank account details);
- if data has been lost or stolen, is there any protection in place such as encryption?
- what has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the information relates; if it has been damaged, this poses a different type and level of risk;
- what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of data could help a determined fraudster build up a detailed picture of other people;
- how many people are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment;
- who are the individuals whose data has been lost, damaged or stolen? Whether they are staff, customers, clients or suppliers will to some extent determine the level of risk posed by the breach and, therefore, the actions in attempting to mitigate those risks;
- what harm can come to those individuals? Are there risks to physical safety for example if an individual is fleeing from domestic abuse? Or risks to reputation, or the possibility of financial loss or a combination of these and other aspects of their life? If individuals' bank details have been lost, consider contacting the banks for advice on anything that can be done to help prevent fraudulent use;

- are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service?

Notification/reporting of breach

6.1 Notification should have a clear purpose, whether this is to:

- enable individuals who may have been affected to take steps to protect themselves;
- ask third parties such as the police, insurers, bank or credit card companies to assist in reducing risks;
- allow the appropriate internal departments to change working practices, perform duties more securely, provide advice and deal with complaints.

6.2 The following prompts will help determine if it is appropriate to notify individual data subjects (or owners):

- are there any legal or contractual requirements for notification or sector specific regulators that require notification?
- will notification help meet security obligations in relation to the seventh data protection principle - *appropriate technical and organisational measures…taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*?
- can notification help the individual? Could individuals act on the data you provide to mitigate risks, for example by cancelling a credit card or changing a password?
- if large numbers of people are affected, or there are very serious consequences, seek advice about informing the Information Commissioners Office (ICO) from your Information Governance lead;
- consider how notification can be made appropriate for specific groups of individuals, for example, if you are notifying children or vulnerable adults;
- consider the dangers of 'over-notifying'. Not every incident will warrant notification and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work.

6.3 What to include in the notification:

- a description of how and when the breach occurred and what data was involved;

- details of steps already taken to respond to the risks posed by the breach;
- specific and clear advice on the steps they can take to protect themselves;
- contact details for further information, questions or queries.

6.4 Where a significant data breach is identified (the data lost is likely to result in a risk to the rights and freedoms of individuals) there is a responsibility for the controller to notify the Information Commissioners Office within 72 hours.

Response, evaluation and review

7.1 It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the response.

7.2 A full report should be prepared by the investigator, authorised by a senior manager and lodged with the information governance lead. This should provide assurance to the subject, management and the ICO of the commitment to information security by the organisation.