Information Sharing Agreement

Safeguarding in Walsall

Part A: The parties' details

Walsall Metropolitan Borough Council

Walsall CCG

Walsall Health Trust

West Midlands Police

Dudley & Walsall Mental Health Trust

National Probation Service

Community Rehabilitation Service

Document Control Page

Version	Date	Changes Made	Change Author
0.1			
0.2			
0.3			
0.4			

CONTENTS

.

Document Control Page 0
1. Purpose of the Agreement 2
2. Policy Context 2
3. Scope 3
4. Purposes for Sharing Information 4
5. Consent 5
6. Legislative Context 5
7. Conditions for Processing Data 5
8. Security Measures 5
9. Storage of Information 6
10. Retention and disposal 6
11. Monitoring and Review 7
12. Reporting and Managing Breaches 7
13. Indemnity Clause 7
14. Warrant and Wavier 8
15. Conclusion 8
16. Approval 8
Appendix A – Details and Purpose of Information being shared 11
Appendix B – Articles 6 and 9 of the General Data Protection Regulations 2016 12
Appendix C – Key Legislation 13
Appendix D – Organisational Policies 15
Appendix E – Glossary 16

1. Purpose of the Agreement

1.1. This Information Sharing Agreement (ISA) defines the arrangements for processing data between the named organisations, hereafter referred to as "Partners or the "Safeguarding Partners" to facilitate and govern the efficient, effective and secure sharing of good quality Information for the purposes of complying with our safeguarding obligations and duties as set out in **Appendix A** for the provision of Safeguarding within Walsall. It also defines the arrangements for safeguarding partners to share information with the Safeguarding Boards

1.2. It sets out:

a) The principles underpinning information sharing
b) The general purposes for information sharing
c) The responsibilities and commitments of partners to this agreement.
d) The arrangements for monitoring and review.

1.3. It is recognised that as policy develops and implementation arrangements mature or legislation changes, this agreement will need to be reviewed and amended in light of new information sharing requirements to ensure that it is 'fit for purpose'.

2. Policy Context

2.1. In order for the development of the Safeguarding to be successful it is essential that Safeguarding Partners are empowered to share good quality and relevant information in a responsible and secure way.

2.2. This Information Sharing Agreement will designate the roles and responsibilities for the above named organisations/Partners in use of the information held on any system for any historical information and new information relating to a person's safeguarding. This ISA will allow authorised staff and partners to share information to improve the quality of data and reporting, assist in safeguarding, tracking and tracing of children and access to the required records, to provide on-going health and childcare services to those in need of our safeguarding services as set out in **Appendix A**.

2.3. Information will be shared jointly between Safeguarding Partners in relation to the above.

2.4. For the purposes of this agreement the following relationships are established;

a) All organisations and members who sign up to this agreement. The signatory organisations as Safeguarding Partners to ensure that there are sufficient security guarantees in place to protect data being shared under this Agreement and to ensure that the sharing of data and ownership meets the requirements of the Data Protection Principles contained in the Data Protection Act 2018 and the General Data Protection Regulations 2016.

b) The Safeguarding Partners will have the status of "Data Controllers in Common" for the purpose of continuous safeguarding delivery, once Safeguarding Partners share and exchange the required level of data

each becomes the data controller of the information they have been provided with under this agreement.

c) The Safeguarding Partners will have the status of Joint Data Controllers in respect of any documentaction which is created jointly by the Safeguarding partners. This documentation will be held jointly by the Safeguarding Partners and any decisions relating to the use of this documentation, including but not limited to the retention and deletion, and further sharing with other third parties, will be taken by the Safeguarding partners jointly.

3. Scope

3.1. This ISA covers the sharing of information between authorised services within your organisation as a safeguarding partner engaged in/or who are identified as holding relevant information for the purposes of;

a) Direct provision of safeguarding and or associated services

b) Supporting the identification of living individuals that require safeguarding services or interventions.

c) Supporting the identification of records required in support of the functions of the safeguarding board.

d) To safeguard identified children and adults under the multi-agency sharing hub and in compliance of the relevant legislation for safeguarding.

e) To support the accuracy of demographic details.

3.2. Accurate, identifiable information is required from our partners to provide support in the delivering of direct safeguarding services to identified individuals and families and to carry out the following functions:

- To obtain assurance that appropriate safeguarding arrangements are in place as required by legislation and statutory guidelines;
- To obtain assurance that the safeguarding arrangements are appropriate and operating efficiently;
- To monitor and oversee safeguarding practice to ensure that there is a culture of accountability and continuous improvement.

3.3. Articles 6 and 9 of the General Data Protection Regulations (2016) (GDPR) set out the conditions for processing and thus transferring when both Personal Data and Special Category Data is involved and is defined in Appendix B.

3.4. Article 10 of the GDPR requires any criminal conviction data to be processed either in an official capacity or in accordance with a condition under Schedule 1, Part 3 of the Data Protection Act 2018 and is defined in Appendix B

4. Purposes for Sharing Information

4.1. Effective information sharing is fundamental to supporting intelligence and providing an evidence base on which all partners can make informed decisions in order to safeguard the welfare of children and adults at risk of harm.

4.2. Legislation including, but not limited to the Children Act 2004, Safeguarding Vulnerable Groups Act 2006,and the Care Act 2014 requires each local authority to promote cooperation with its partner agencies, with a view to improving and protecting the well-being of children and adults in its area. Well-being is defined by the act as relating to:

- physical and mental health and emotional well-being
- protection from harm and neglect
- education, training and recreation
- the contribution made by them to society and
- social and economic well-being

4.3. This agreement will assist sharing to allow the Safeguarding Partners to meet the following safeguarding obligations:

- **Risk assessment and decision making.**

  Using the best information available to the partnership to identify those children and adults who require support and to assess their needs.

- **Identification of concern.**

  Using the best information available to the partnership to identify children and adults at risk of, or experiencing, serious harm or who are likely to experience future harm without intervention and support.

- **Service provision and harm reduction.**

  Using the best information available to the partnership to develop a proportionate response to the needs of children and adults at risk of harm, including harm reduction strategies and early help.

4.4 The agreement will enable the sharing of Personal Confidential Data (PCD) between partners delivering public services in order to:

- Provide appropriate care services and support people in need.
- Safeguard rights to confidentiality for the public and staff.
- Ensure the effective management of information in order to develop and deliver plans and strategies required by central government.
- Allow the effective flow of information between partners to assist with the development and delivery of plans developed by partners and inter organisational strategies
- Enable the investigation of complaints or serious incidents

- Enable partners to fulfil their legal obligations (see Appendix C - Key Legislation)

5. Consent

5.1. Where consent is required it is the responsibility of the relevant Data Controller to seek consent from their clients to share information for any purposes that fall outside of the scope and requirements for the sharing of data as identified in this agreement.

5.2. It likely that consent will not be obtained, dependent on the nature of the Safeguard concerns being raised.

5.3. At all times, joint data controllers will keep accurate records that justify why consent may not have been obtained. That includes who made the decision to share information and the basis for deciding to share.

6. Legislative Context

6.1. It is essential that all information shared under the terms of this agreement will be done so in compliance with the following key legislation. See **Appendix C**

7. Conditions for Processing Data

7.1. The GDPR states that personal data shall: be processed fairly and lawfully and, in particular, shall not be processed unless a condition in Article 6, and for special category data, a condition in Article 9 are met below, see **Appendix B**

7.2. The information should only be used for the specified purpose in this agreement and not for any purposes outside of the safeguarding requirements without consent from the partner who originally shared the information, or where required the data subjects directly.

7.3. All identifiable data is classed as personal confidential and sensitive. Therefore if any identifiable data is to be shared, an Article 6, and for special category data, an Article 9 condition must be met, see **Appendix B.**

7.4. Article 10 (criminal history) may also apply.

8. Security Measures

8.1. The Safeguarding Partner organisations have Data protection, Information Security and Confidentiality Policies containing the principles of that Data Protection Act 2018 and or the General Data Protection Regulations, Caldicott Principles, NHS Confidentiality Code of Practice and NHS Records Management Code of Practice, or the Public Records Act. These policies are listed at **Appendix D**.

8.2. Where data transfers and sharing is concerned each organisation will ensure that an agreed and appropriate secure method of data transfer can take place that is agreed by all partners to this agreement. This meets the requirement to ensure that appropriate levels of security are applied at all times to the level and category of data being shared.

9. Storage of Information

9.1. Each individual Safeguarding Partner takes responsibility for ensuring that any information shared with them is stored securely and appropriate technical and organisational methods are implemented to protect the integrity of the information.

9.2. Information that is shared with its Safeguarding Partners will be stored appropriately in compliance of the Data Protection Act 2018 and or GDPR and any future legislative requirements as is the duty of a Data Controller.

9.3. The individual Safeguarding Partners must have appropriate security and access controls in place as is required under the duties of a data controller.

10. Data Subject Rights

10.1 Each party to this agreement retains responsibility for responding to Freedom of Information and Subject Access Requests.

10.2 Each party to this agreement is responsible for ensuring that any amendments to data in accordance with Articles 12 – 22 of the GDPR are communicated to the Safeguarding Board.

10.3 Any notification under clause 10.2 should be made to the Safeguarding Board Business Manager in the first instance.

10.4 Any request (e.g. Freedom of Information) relating to records created by the Board will be managed by the Board Business Unit. All parties to the agreement will work together to support the Business Unit in managing and responding to these requests.

10.5 Notification of a serious incident which may lead to a referral for a statutory review should be made to the Business Manger as soon as possible and the referral made in line with the procedure for Adults or Children's .

11. Retention and disposal

11.1. Each party to this agreement should have an appropriate retention policy to ensure information and documents are only kept for as long as is necessary.

11.2. As Data Controllers in common each party to this agreement will ensure that any shared data and or records are held, archived and deleted accordingly in line with the local, national and legal requirements including but not limited to;

- the Public Records Act;
- the Records Management Code of Practice for Health and Social Care;
- the Health and Social Care Act

- the Local Government Act

12. Monitoring and Review

12.1. The ISA will be monitored and reviewed annually for any changes required. All amendments to this ISA will be reported to and signed off by the Caldicott Guardian, Senior Information Risk officer (SIRO) or Data Protection lead (DPO) of each Safeguarding Partner and upon approval of the respective Information Governance Committees.

13. Reporting and Managing Breaches

13.1. Any data breach must be reported to the Data Protection Officer of the organisation responsible for the breach immediately, or within 24 hours of the incident, giving the details of the breach or near miss. Such notifications shall be between respective Information Governance Departments within each organisation.

13.2. All serious incidents must be reported to the ICO by the relevant Data Protection Officer with 72hours.

13.3. The Data Protection officer of the organisation responsible for the breach must inform the Safeguarding Board (via the Business Unit) so that they can take appropriate steps, including notifying the other Safeguarding Partners if this is appropriate.

14. Indemnity Clause

14.1. The Safeguarding Partners agree to indemnify each other in the following terms.

14.2. To ensure that the liability for any breach of this ISA rests with the organisation responsible for that breach alone, the Partners will not accept liability for any loss, unauthorised breach of confidentiality or any breach of terms of this agreement by any employee of another Partner, including the following acts or omissions:

a) Requests for and disclosure of information for purposes other than those specified in the agreement.
b) Use of the information for purposes other than those specified in the agreement.
c) Disclosure of the information to a third party except as specified in the agreement.
d) Handling, recording, storing or disposal of information otherwise than in accordance with the agreement whether negligently or otherwise.
e) Loss or compromise of the information.

15. Warrant and Wavier

15.1. Each party to this agreement is responsible for their own adherence to data protection legislation.

15.2. The parties agree to jointly review this agreement and all sharing arrangements in the event of a data breach

16. Conclusion

16.1. This ISA proposes a consistent approach to the sharing of information between Safeguarding Partners for the purposes of delivering and upholding high quality Child Health Information Services as set out in **Appendix A**.

16.2. All parties need to be able to balance the conflicting demands between the need to share information with other agencies and the requirement to maintain confidentiality. These conflicting demands are acknowledged by this protocol which provides a basis for partners to be confident that where information is shared it will be done in a consistent, responsible and secure way for the purpose of safeguarding children and vulnerable adults.

17. Approval

17.1. The parties to the Agreement accept that the procedures within it will provide a secure framework for information sharing in a manner compliant with their statutory and professional responsibilities.

IN WITNESS WHEREOF:-

On behalf of Walsall Metropolitan Borough Council the following authorised signatories agrees to the terms set out in this Agreement.

Name: Stephen Gunther

Position: Caldicott Guardian

X _____

Stephen Gunther
Caldicott Guardian

Date_____.

_____

Name: Sally Rowe

Position: Executive Director Children Services

X _____

Sally Rowe
Executive Director Children Services

Signed for and on behalf of xxxxx **by its authorised signatories:**

Name:
Position: Caldicott Guardian

_____

Name:
Position:

Appendix A – Details and Purpose of Information being shared

Purpose	Type of Information	Recipients
Delivery of Safeguarding Services in compliance with the Children Act 2004, Safeguarding Vulnerable Groups Act and the Care Act 2014	Client user records including • Name • Address • Gender • Ethnicity • D.O.B • Details of engagement by individual with services offered or withdrawn	Members of the Safeguarding Board and other relevant partners as identified: Walsall Council Walsall CCG West Midlands Police Walsall Healthcare Trust Dudley and Walsall Mental Health trust Black Country Partnership Foundation Trust Schools / educational establishments / early years providers Primary Care facilities Healthwatch Probation West Midlands Fire Service West Midlands Ambulance Service Commissioned services

Appendix B – Articles 6 and 9 of the General Data Protection Regulations 2016

Article 6- Personal Confidential Data		Article 9 – Personal Sensitive Data	
a) The individual who the personal data is about has consented to the processing.	✓	a) The individual who the sensitive personal data is about has given explicit consent to the processing.	✓
b) The processing is necessary: - In relation to a contract which the individual has entered into; or - Because the individual has asked for something to be done so they can enter into a contract		b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law	
c) The processing is necessary because of a legal obligation that applies to the Trust/Local Authority (except an obligation imposed by a contract).	✓	c) The processing is necessary to protect the vital interests of: - The individual (in a case where the individual's consent cannot be given or reasonably obtained), or - Another person (in a case where the individual's consent has been unreasonably withheld)	✓
d) Vital interests of the data subject. This condition only applies in cases of life and death, such as where an individual's medical history is disclosed to an A&E department treating them after a serious road accident.		d) The processing is carried out by a not-for- profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.	
e) The processing is necessary for exercising statutory, governmental, or other public functions.	✓	e) The individual has deliberately made the information public.	
f) The processing is in accordance with the "legitimate interests" condition.		f) The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise establishing, exercising or defending legal rights.	
		g) Processing is necessary for reasons of substantial public interest.	✓
		h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.	✓
		i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.	
		j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)	

Appendix B – Article 10 of the GDPR

Article 10 – Criminal Conviction Data	
The data is processed in an official capacity.	✓
The data is processed in accordance with Schedule 1, Part 3, Para 36 of Data Protection Act 2018 - the processing would meet a condition in Part 2 of this Schedule but for an express requirement for the processing to be necessary for reasons of substantial public interest.	✓

Appendix C – Key Legislation

- Adoption and Children Act 2002;
- Anti-social behaviour, Crime and Policing Act 2014
- Care Act 2014
- Care Planning, Placement and Case Review and Fostering Services (Miscellaneous Amendments) Regulations 2013
- Care Standards Act 2000
- Children Act 1989
- Children Act 2004
- Children and Adoption Act 2006
- Children and Families Act 2014
- Children and Social Work Act 2017
- Children and Young Persons Act 2008
- Children (Leaving Care) Act 2000
- Crime & Disorder Act 1998
- Criminal Justice and Courts Act 2015
- Data Protection Act 2018
- Disability and Discrimination Act 2005
- Domestic Violence Crime and Victims Act 2004
- Domestic Violence Protection Orders 2014
- Education Act 2002;
- Education Act 2011
- Equality Act 2010
- Education (SEN) Regulations 2001
- Female Genital Mutilation Act 2000
- Forced Marriage (Civil Protection) Act 2007
- Fostering Service Regulations 2011
- Health & Safety at Work Act 1974
- Health and Social Care Act 2012
- Human Rights Act 1998
- Local Authority Social Services Act 1970
- Learning and Skills Act 2000
- Mental Capacity Act 2005,
- Mental Health Act 1983/2007
- Modern Slavery Act 2015.
- National Health Service Act 2006
- Serious Crime Act 2015
- Public Interest Disclosure Act 1998
- Preventing and Combating Violence against Women and Domestic Violence Act 2017
- Safeguarding Vulnerable Groups Act 2006
- Sexual Offences Act 2003
- The Police and Justice Act 2006

Appendix D – Organisational Policies

A Walsall Metropolitan Borough Council

a) Information Governance Framework

b) Corporate Retention Schedule

c) Mobile Device Acceptable Use Procedure

d) Child Care Manual

B Your Organisation Name

a) Insert relevant Policy details here

Appendix E – Glossary

"Confidential Information":

Any information or combination of information that contains details about an organisation or an individual person that was provided in an expectation of confidence. This includes for example, non-personal corporate or technical information that is commercially sensitive, drafts of documents that are not ready for publication, restricted information and documents, etc. as well as personal data about patients, service users and staff.

"Consent (Informed)":

Consent must be freely given, specific, informed and unambiguous for each purpose for which the data is being processed.

"Data/Information":

Means any information of whatever nature that, by whatever means, is shared.

"Data Controller":

As defined in the General Data Protection Regulations 2016 (GDPR) is the individual or organisation (legal entity) who determines the manner and purpose of the processing of the personal information, including what information will be processed and how it will be obtained.

"Data Protection Principle":

Shall have the same meanings as are assigned to those terms in the GDPR;

"Development":

A process by which a cause/service/ system will grow and become advanced.

"Direct Care:

A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of an identified individual

"Evaluating":

Assessing if the system/service being provided is productive and efficient.

Record":

a document in either paper or electronic format which is used to hold and collect information about the health and wellbeing of a

data subject in order to facilitate their care and treatment by health care professionals.

“ICO”:

Information Commissioners Office / The Information Commissioner

“Implementing”:

A process by which a system/service is put into practice/action to develop.

“Monitoring”:

Observe and check the progress or quality of (something) over a period of time; keep under systematic review.

“Personal Data”:

Any factual information or expressions of opinion relating to an individual who can be identified directly from that information or in conjunction with any other information that is held by or comes into the possession of the data controller.

“Processing”:

in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data,

“Special Category Data”:

The categories of personal information defined as special category personal data in Article 9 of the GDPR and, in this Agreement specifically including (but not limited to) information about the physical and mental health, racial or ethnic origin, sexual life or sexuality of patients or service users.