



Walsall Schools Information Sharing Protocol

Introduction

The Council, educational establishments and our partners such as the Police, CCG, Health Trust and Safeguarding Board within the borough frequently need to share personal information on a daily basis in order to appropriately carry out our functions and comply with any obligations placed upon us. This Protocol sets out the overarching Data processing and information sharing principles between Parties in sharing Data between the organisations. Walsall Council will be responsible for the publication, maintenance and regular review of this document. Walsall Council will ensure that a list of signatories is published and will be responsible for making sure that this is kept up to date.

This Protocol applies to all public sector organisations, third sector organisations and those private sector organisations contracted to deliver services to the public sector and who provide services involving the health, education, safety, crime prevention and social well-being of people in Walsall and the surrounding areas. It particularly concerns those organisations who hold information about individuals and may consider it appropriate to share the information with others.

Educational establishments, including maintained schools, are independent from the local authority for the purposes of data protection legislation and all parties to this agreement are Data Controllers in their own right. Prior to sharing any information under this protocol, each organisation is responsible for ensuring that the proposed recipient of the data is a signatory to this agreement. If the recipient is not a signatory then alternative agreements may be required by the parties.

Sharing information is necessary to ensure that public services are delivered efficiently and effectively to meet the needs of residents and service users.

This Protocol is intended to help ensure compliance with the statutory and legislative requirements relating to the disclosure of personal information including the General Data Protection Regulations (2016), the Data Protection Act 2018, the Human Rights Act 1988 and the common law duty of confidentiality.

By agreeing to be part of this Protocol, which is intended to provide openness and transparency for Data sharing arrangements, we consider it will provide both appropriate governance and support to you in fulfilling your duties as the 'Data controller' for your institution, ensuring the safe, lawful and secure sharing of personal Data. This has been reviewed to align with updated guidance issued by the Information Commissioner's Office ('ICO').

In signing up you agree to share and receive Data in accordance with the standards defined within this protocol.

This Protocol will cover the following:

- Sharing between Parties as Data Controller(sharer) to Data Controller(recipient);
- Sharing between Parties as Joint Data Controllers;



- Sharing between Parties for the purposes of a Data processing arrangement.

The conditions and requirements within this Protocol will apply to all staff, agency workers, volunteers and any other working on behalf of the partner organisations including agents and sub-contractors.

The Protocol will be reviewed annually, by the relevant service area within WMBC, in order to ensure it meets the Data protection legislative requirements.




Signed on behalf of Walsall Council:

Signature:

Sally Rowe

Executive Director of Children's Services

Date: 07.03.2019

Signature: 

Paul Withers

Data Protection Officer

Date: 07.03.2019

Signature: 



Walsall Council

Signed on behalf of

Name of Organisation:

Name:

Position:

Signature:

Date:



WORD/PHRASE	DEFINITION
Controller	As defined in Article 4 of the GDPR.
Data	as defined within the GDPR and the DPA, including both Personal and Sensitive Data, and also any Data which is not defined by the DPA and which comprises any written information which is provided to or acquired by the Parties which is either (a) commercially sensitive, or (b) confidential, or (c) Special Categories of Personal Data and (d) 'information asset'
Data Protection Legislation	<p>The statutes, regulations, codes and guidance to include (but limited to) the following:</p> <ul style="list-style-type: none">i) The General Data Protection Regulation (Regulation (EU) 2016/679) (the 'GDPR');ii) The Data Protection Act 2018 and any subsequent Data Protection legislation (the 'DPA');iii) The EU Data Protection Directive 95/46;iv) The Regulation of Investigatory Powers Act 2000;v) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;vi) The Electronic Communications Data Protection Directive 2002/58/EC;vii) The Privacy and Electronic Communications (EC Directive) Regulations 2003;viii) All applicable laws, and regulations relating to the Processing of Data and privacy including (where applicable and without limitation) the guidance and codes of practice issued by the Information Commissioner under the GDPR, DPA and under any subsequent Data Protection legislation. <p>This will also include any statutes, regulations, codes and guidance which may come into force at a future date.</p>
Data Subject	The identifiable natural person to whom the Personal Data belongs
DPA	The current Data Protection Act 2018 and any subsequent Data Protection Legislation.
DPO	Data Protection Officer



Fair Processing Notice	Information provided to the individual either when collecting the information, or at the point of receipt of the information from a third party. This notice must comply with the requirements of Articles 12, 13 and 14 of the GDPR and any relevant Data Protection Legislation.
Filing System	Any structured set of Data which is accessible according to specific criteria, whether centralised, de-centralised or dispersed on a functional or geographic basis
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679)
ICO	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. The UK independent authority for regulating and monitoring activity under all relevant Data protection and information rights legislation.
In Writing	Any reference to 'in writing' or 'written' shall be construed to mean to trace or form or transcribe (characters, letters, words etc.) on paper and or in electronic formats, such as in letters, records or in email that captures information that falls under the processing conditions of this Protocol.
Information Asset Owner	A designated senior officer with ownership and responsibility for specific information assets (including paper based and electronic records and IT systems)
Joint Controllers	As provided in Article 26 of the GDPR
Party/Parties	The organisations who have signed up to this Protocol.
Personal Data	As defined in Article 4 (1) of the GDPR
Personnel	All employees of the Processor, or its suppliers, contractors, sub-contractors, officers, agents, students on work experience and volunteers who are from time to time employed and/or engaged in connection with processing Data on behalf of the Data Controller or otherwise in relation to the performance of a contract.
Privacy Notice	This shall have the same meaning as Fair Processing Notice.
Processing / Processed / Process	The definition for Processing/Processed/Process within this Protocol shall have the same meaning as Processing within Article (4) (2) of the GDPR
Processor	As defined in Article 4 of the GDPR
Protocol	This document and all of its schedules and any variations to it. All Parties to the Protocol must agree any variations in writing.



Walsall Council

Working Days	Any day that is not a Saturday, Sunday or public holiday in England.
--------------	--



1. Purpose for sharing Data

Effectively sharing information will bring significant benefits in supporting the learning, welfare and safeguarding of children and young people in Walsall.

Information will be used to plan and deliver services and support decision making on a case-by-case basis. Sharing Data will enable services to be targeted and delivered effectively.

This protocol is designed to cover sharing between organisations and there is no requirement under this Protocol to implement an information sharing agreement for information that is disclosed or exchanged on an ad-hoc or infrequent basis.

It may be determined that an individual information sharing agreement may be appropriate or necessary for a specific projects which required disclosure of information between two or more parties. In this situation, the information sharing agreement will be supplemental to this Protocol and should incorporate the provisions of this Protocol.

2. The information sharing partner organisations

Each party who agrees to adhere to these provisions will be required to sign the up to the Protocol. A list of the signatories can be found in Appendix 1.

Formal adoption must be determined and agreed at Senior Management level as appropriate to each organisation.

Every organisation should nominate a point of contact / owner who takes responsibility for ensuring that this Protocol is understood and followed within their respective organisations.

The organisations who may sign up to this agreement include but are not limited to:

- Maintained Schools, Academies and Higher Education Providers within Walsall
- West Midlands Police
- Walsall Health Trust
- Walsall CCG
- Walsall Safeguarding Board
- Walsall M.B.C.

3. Data being shared

Information will be shared between partner organisations to achieve the following objectives:

- Ensuring sufficient and appropriate learning provision;
- Supporting Education Provider(s) improvement and improved educational outcomes through pre and post 16 learning;
- Ensuring effective planning, commissioning and delivery of services to Young People and families, in particular to support vulnerable Young People and their families.
- To fulfill our obligations with regard to safeguarding and social protection;
- To carry out consultation and continually improve our services;



- To carry out the statutory and regulatory functions;
- To meet legal requirements and comply with legal obligations;
- To comply with our Public Health functions by sharing Health and other relevant data;
- To prevent or detect crime and fraud and to protect individuals from harm;
- To fulfil key strategic responsibilities;
- To support the work of Community Partnership Group

Some Data will be shared in order to fulfil contractual obligations when an Education Provider purchases a traded service from WMBC. When an education provider purchases a traded service from WMBA, the education provider will be the Data Controller and WMBC will be their Data Processor. In these circumstances WMBC may only process Data in accordance with the written instructions of the Education Provider under the terms of the specific "Service Level Agreement" (SLA) and or contract and in accordance with the data protection legislation.

4. Legal basis for sharing information

Personal Data should be shared fairly and lawfully. In order to achieve this, Parties must comply with at least one condition from Article 6 and, where special category (sensitive) information is included, at least one condition from Article 9 of the GDPR.

Article 6	Processing of Personal Data
6a	Consent: the individual has given clear consent for you to process their personal Data for a specific purpose.
6b	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.
6c	Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
6d	Vital interests: the processing is necessary to protect someone's life.
6e	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.

Article 9	Processing of Special Category – Sensitive Data
9a	the Data subject has given explicit consent to the processing of those personal Data for one or more specified purposes
9b	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
9c	processing is necessary to protect the vital interests of the Data subject or of another natural person where the Data subject is physically or legally incapable of giving consent;



9g	processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued
----	---

Fair processing is the responsibility of each Controller to ensure by the issuing of a Privacy Notice that all Data subjects are aware of how and when their Data is processed.

If the information sharing is based on consent, relevant Parties to this must ensure that it is explicit, affirmative consent and meets the definition given in the GDPR. There must also be appropriate mechanisms in place to record any retraction of consent and cease the sharing of the Data.

5. Access and individual's rights

The Parties acknowledge that Data subjects have rights under Articles 12 through to Article 22 (inclusive) of the GDPR. The Parties will deal with the exercise of subject rights in accordance with the requirements of the GDPR and relevant Data Protection Legislation. All organisations must have appropriate policies and procedures in place which allow these rights to be exercised by the data subject. The Parties undertake to keep each other advised of the exercise of subject rights in relation to Data shared under this Protocol

To comply with fairness and transparency requirements, it is the responsibility of each Party to ensure that their Privacy Notice(s) or fair processing notice(s) properly reflect their Data sharing arrangements in accordance with the requirements of Articles 13 and 14 of the GDPR.

Freedom of Information Act 2000 (FOI) requests and data protection subject access requests:

- Any request for information made under the Freedom of Information Act must be notified to the Party who is the Controller of the Data, within 3 working days, in order to fulfil the 20 working days FOI legislation.
- Any subject access request made under Data Protection Legislation must be notified to the must be notified to the Party who is the Controller of the Data, within 3 days, in order to fulfil the 30 day GDPR legislation.

Where a subject access request involves Data received from another Party, the receiving Party shall determine whether they need to contact the Party who initially shared the Data to advise them accordingly and seek any representations, including whether, for example, an exemption to disclosure would apply. However, the decision to disclose rests with the receiving Party.

Where a Data subject exercises their right to rectification, erasure or restriction with regard to Data shared under this Protocol, the Party who shared the Data must notify the receiving Party and or Parties as soon as is practicable of the outcome of the request. The Parties who received the Data under this Protocol must have appropriate mechanisms and procedures in place to effect any amendments required, including the addition of a supplementary statement.

Where a Data subject exercises their right to rectification, erasure or restriction with regard to Data received from another Party under this Protocol, the receiving Party must notify the sharing Party as soon as is practicable and without undue delay. The Party who received the Data under this Protocol shall use best endeavours to assist the Party who provided the Data in complying with any investigation, actions or requirements.



Where a Data subject exercises their right to rectification, erasure or restriction with regard to Data received from another Party under this Protocol, the Party who received the Data must be able to comply with Article 19 of the GDPR. They must ensure they have appropriate mechanisms in place to be able to communicate the outcomes and requirements of this to any third party they have disclosed the information to.

Where a Data subject exercises their right to object, the Party receiving the complaint shall notify the DPO of the relevant Party by the following working day. All Parties must have appropriate mechanisms and procedures to cease processing of the specified Data whilst the validity of the request is assessed. If the request is upheld there must be no further processing of the Data.

Where any complaint or claim that there has been a breach of any of the Data subject's rights or the Controller obligations, the Party receiving the complaint shall notify the DPO of the organisation who initially shared the data immediately. Notification may be by telephone or email and use best endeavours to assist in complying with any investigation, actions or requirements of such complaints or breaches.

This Protocol is not confidential and will be available for anyone to view.

6. Keeping Data secure and confidential

Each organisation should have policies and procedures in place which govern the processing of information and ensure that all activity is undertaken in accordance with the principle of integrity and confidentiality under Article 5 of the GDPR.

Each organisation shall implement appropriate technical and organisational measures to protect the Data from any unauthorised or unlawful Processing or accidental loss, destruction or damage in line with the obligations of a Data Controller. These measures must be:

- a. compliant with national Data security requirements, standards and or certification such as ISO/IEC 27001:2005 (ISO/IEC 17799:2005) as appropriate to the Data being shared under the Protocol; and
- b. fully and diligently complied with by its Personnel at all times; and
- c. compliant with and meets the requirements of the Data Protection Legislation.

Each organisation will ensure that their Personnel, including temporary and contract employees, are able to access only the shared Data necessary for their role.

Each organisation will ensure that their Personnel, including temporary and contract employees, are subject to appropriate confidentiality and non disclosure obligations.

Each organisation will ensure that their Personnel, including temporary and contract employees, and are appropriately trained so that they understand their responsibilities for confidentiality and privacy.

Each organisation must give consideration to the extent of any Personal Data that is disclosed. Only share relevant Data to fulfil the objective of the sharing.

Each organisation must protect the physical security of the shared Data.

Each organisation shall ensure that electronic copies of the Data are only ever held on encrypted devices or servers and are not e-mailed un-securely. Any portable devices must be encrypted and Data should not be transferred onto unsecure portable devices. When Data is



no longer required it must be disposed of securely and permanently in accordance with this Protocol and or any binding retention or archiving requirements and or codes of practice.

Each organisation shall ensure that all paper copies held by it of any Data are held securely and transferred either by safe haven fax or couriered in sealed containers and shredded upon disposal.

Personal Data must only be sent via encrypted email such as GCSX or future designated secure platforms to be agreed between Parties.

No Parties may pass on the Data to other third parties without an appropriate lawful basis under GDPR. If Data is shared with third parties who are not a party to this Protocol, the sharing Party is responsible for ensuring that there are appropriate Data sharing arrangements and it is done in accordance with the requirements of the GDPR and Data Protection Legislation.

Each organisation are responsible for ensuring that there are appropriate Data processing agreements in place if third party Processors are used. Any Data processing agreements must ensure there are sufficient provisions to meet the GDPR requirements and protect Data subject rights. All Parties are required to ensure any sub-contractors they use are managing all aspects of Data security and are fully aware of and abide by this Protocol.

Any Data breaches involving data shared under this protocol for example: theft, loss, damage or inappropriate disclosure of Data must be reported to DPO of the organisation who originally shared the information.

7. Record of Processing Activity

Any request to share information must clearly state the following:

- the information required;
- the purpose for sharing and intended use of the data;
- the lawful basis for sharing;

Each organisation is responsible for keeping appropriate records of Data Processing activity, including the sharing of Data pursuant to this Protocol.

8. Data retention and deletion

The Data will be retained in accordance with the Data Protection Legislation requirements and organisational guidance. Each organisation must have an appropriate retention schedule in relation to the retention and deletion of Data.

Subject to any statutory retention requirements, once the reasons for sharing the Data have been satisfied the Data will be securely destroyed. All relevant Data must be deleted from computer systems (including, but not limited to; personal computers, laptops, other computers, electronic handheld devices, memory sticks, USB sticks, servers, hard drives, CD ROMs, and other forms of media storage inclusive of cloud storage) and any hard copies destroyed.

9. Responsibility for exchanging the Data and ensuring Data is accurate



All Data received by Parties, must be stored, retained and disposed of in line with their own records retention and security policies which must comply with the requirements of the GDPR and Data Protection Legislation.

Each organisation is responsible for ensuring that they have appropriate safeguards in place to ensure that any shared Data is accurate.

If Data is found to be inaccurate, it is the responsibility of the organisation who discovered the inaccuracy to notify the organisation who shared the Data. The organisation who originally shared the Data will ensure the Data is corrected and will notify all other parties.

10. Complaints

Parties to this Protocol will use their standard organisation procedures to deal with complaints from the public arising from sharing Data under this Protocol.

11. Data Breach

If a Data breach is found to have occurred, it is the responsibility of the organisation who becomes aware of the breach to notify the organisation who is Controller of the Data which has been breached, who will ensure the Data breach is reported appropriately and the necessary reporting requirements and timescales are adhered to.

Each organisation is responsible for having appropriate measures in place to manage Data security breaches including identifying, investigating and dealing with unauthorised access to, or use of, Data whether intentional or inadvertent. Each organisation will undertake to advise the other immediately in the event of a Data security breach affecting Data shared under this Protocol.



Appendix 1 – Signatories

Information Sharing Partner Organisations Signature	
[Insert organisation name here]	[Insert ISP owner / point of contact]
[Role]	[Date]
[Signature]	

As signatures are returned using the separate signatures sheet they will be collated here and once complete a fully signed version will be publicly available via the Walsall Link web portal.