**Tier 1 Information Sharing Agreement**

# 1 Introduction

1.1 This agreement aims to provide the organisations outlined in section 12 of this Agreement, with a robust foundation for the lawful, secure and confidential sharing of personal data (Information) between themselves and other public, private or voluntary sector organisations that they currently work with or might work with in the future, with respect to the provision of services for customers of the partner organisations.

1.2 This agreement will assist all partners to meet their statutory obligations and to share information safely to facilitate the integration of service provision between the partner organisations.

1.3 This agreement aims to support the following:

* Collaborative working;
* Integrated working;
* Implementation of new and national initiatives;
* Quality and audit processes;
* The health, safety and well-being of customers and residents;
* Improvement in social housing and related services
* Provision of information (reporting and validation);

# 2 Purpose of the Agreement

2.1 The purpose of this Agreement is to establish a guiding framework to manage exchanges of Information among themselves as partner organisations, taking into account the legal context and basis for sharing Information.

# 2.2 This agreement will:

* Be supported by the use of Tier 2 Information Sharing Agreements (ISA), as set out in Appendix C.
  + A Tier 2 ISA is set up for specific information projects between partner organisations;
* Encourage the sharing of Information between partner organisations where it will support the aims set out above;
* Assist in the development of good practice across partner organisations and their integrated teams;
* Provide the basis for processes which will allow monitoring and review of Information flows and Information sharing between partners, and promote accountability;
* Assist in reducing the risk of unlawful sharing of Information between partner organisations;
* Reduce the need for individuals to provide duplicate Information when receiving an integrated service;
* Reduce the reputational risk to the partner organisations that could be caused by the inappropriate or insecure sharing of sensitive Information; and
* Not be contractually binding but will set good practice standards that the sharing partners are required to meet.

2.3 This Agreement does not imply an obligation on partner organisations to exchange information. Such decisions are subject to the policies and discretion of the signatory organisations.

2.4 This Tier One agreement should not be seen as sufficient in itself or an adequate substitute for a Tier 2 agreement; Tier 2 agreements must be completed for specific information sharing projects between the Partner Organisations.

# 3 Scope

3.1 This Agreement considers the foundation for all personal and sensitive information processed by partners that is shared for the purposes of providing a more seamless service to the individual.

3.2 This Agreement regards all personal information relating to an individual as confidential. Information should only be shared if there is a legitimate purpose, statutory obligation or lawful basis and is covered by associated procedures and/or agreements to this document between partners and/or specific services.

3.3 This Agreement refers to the Data Protection Act 2018 (DPA) for the definition of “personal information” and “data” as any information held either in manual or electronic records including that which is held virtually, on the internet and within social media, or records held by means of audit and/or visual technology about an individual who can be personally identified from that information.

3.4 The DPA further defines certain classes of personal information as Special Categories of Data or sensitive data, for which additional conditions must be met to ensure the information is used and disclosed lawfully. All partners under this Agreement are expected to treat sensitive data in line with the conditions set out by the DPA.

3.5 This Agreement defines processing and sharing of information as collecting, obtaining, recording, organising, discussing, holding, retrieving, altering, analysing, processing, destroying or disclosing data which can be transferred verbally, in writing or through electronic medium including images and photographs.

3.6 Compliance with this Agreement and the Legislative Framework that it seeks to embed in the Partner Organisations is the responsibility of all staff working with or for the partner organisations, including directors, employees, voluntary or contracted staff), to the extent that their roles involve the processing of Information.

3.7 This Agreement does not replace the need to conduct a Data Protection Impact Assessment (DPIA) on the information or processes involved.

# 4 Partnership Agencies Involved

# 4.1 This Agreement requires each participating organisation to have a nominated point of contact and a named deputy who is responsible for:

* agreeing who in their organisation has access to the shared information;
* agreeing amendments to this agreement or any consequential arrangements; and
* ensuring mechanisms are in place to monitor the operation and to ensure compliance with this agreement.

4.2 The following agencies included by this Agreement are listed in section 12, which also includes the details of nominated point of contact.

# 5 Legal Context and Basis for Sharing Information

Set out below is a non-exhaustive list of the legislation and law, compliance with which may provide the Partner Organisations with a lawful basis for sharing Information amongst themselves:

* Housing Act 1985 and 1988. Schedule 2, Ground 2 (Secure Tenancies) and Schedule 2, Ground 14 (Assured Tenancies)
* Housing Act 1996. Section 153, as amended by Section 26, Police & Justice Act 2006. Section 153A: Anti-social Behaviour. Section 153B: Unlawful Use of Premises. Section 153C: Exclusion Orders. Section 153D: a Breach or Anticipated Breach of a Tenancy Agreement
* The Protection from Harassment Act 1997
* Homelessness Act 2002. The Housing Act 1996, as amended by the Homelessness Act 2002 and The Homelessness Reduction Act 2017
* Crime and Disorder Act 1998
* Anti-Social Behaviour, Crime and Policing Act 2014
* Data Protection Act 2018.
* The Civil Evidence Act 1995
* Police Reform Act 2002
* Human Rights Act 1998.
* Common Law Power of Disclosure
* Code of Practice on the Management of Police Information.
* The Housing Benefit Regulations 2006

# 

# 6 Defined Purposes

6.1 With reference to the general principles outlined in Section 7: General Principles, the following justifiable purposes have been agreed by all participating organisations. These are examples are not exclusive or prioritised:

* Prevention and or management of anti-social behaviour
* Investigation of suspected tenancy or benefit fraud
* The provision of services, such as property adaptions assuring and improving the quality of services and social care;
* risk management;
* investigating complaints and notified or potential legal claims;
* managing and planning services;
* contracting for services;
* statistical analysis and reporting;
* where emotional, physical or sexual abuse or neglect are suspected;
* ensuring holistic assessments of vulnerable individuals developmental needs;
* disclosure of information as appropriate for the purpose of legal proceedings in connection with the health and social care of the identified person(s);
* sharing information in relation to carers;

6.2 When sharing information, the organisation should take appropriate, reasonable steps to ensure that the information is accurate, up-to-date and not excessive or irrelevant. Information sharing should be in accordance with:

* Section 8: Parameters; and
* Section 9: Access and Security.

# 7 General Principles

7.1 Any actual or potential breach of information security in relation to data transferred in accordance with any agreement should be reported immediately to the organisation’s key contact in section 12 of this agreement and for them to follow their internal processes for reporting.

7.2 All data subject concerns about the processing of personal data should be addressed by the organisations involved with processing that data, by following their own internal procedures.

7.3 Disclosure of information to third parties not listed as a Partner Agency in section 12 should involve the specific consent of the nominated manager or their named deputy of the organisation originally supplying the information if its disclosure is for purposes other than those for which it was originally collected.

# 8 Parameters

8.1 Transfers should contain no more than the minimum amount of personal information necessary for the task.

8.2 Where information is required for a secondary purpose, pseudonymisation or anonymisation should be applied as appropriate, following advice from the Information Governance Lead or Data Protection Officer in each organisation.

8.3 Specific agreement will be required (from the disclosing organisation’s nominated manager or their named deputy) prior to personal information being transferred for purposes other than those defined in the Agreement.

8.4 Where it is proposed to disclose information received for the purposes defined in this Agreement to organisations that are not listed in Section 12, the following process must be followed:

* Specific agreement will be required from the nominated manager or their named deputy of the originating organisation prior to personal information being disclosed to any 3rd party;
* The nominated manager or their named deputy must ensure that procedures are in place so that disclosures of person-identifiable information are consistent with their organisation’s registration under the Data Protection Act;
* If a disclosure to a third party is outside the originator’s purpose for collection as defined in their Data Protection Act registration, the specific consent of the nominated manager or their named deputy of the originating organisation must be sought;

8.5 Where a data subject should be consulted over the data transfer and is unable to give informed consent, the decision should be made in accordance with the relevant legislation.

8.6 Where practicable, advice should be sought from the nominated manager or their named deputy and the reasons for the final decision should be clearly recorded.

8.7 It is the responsibility of the providing organisation to ensure that the sharing of Information under this Agreement is made in compliance with all its obligations as a Controller under the DPA, with particular regard to the lawful basis and the classification of the Information as Special Category.

8.8 Publishing an accurate Privacy (Fair Processing) Notice is the responsibility of the organisation disclosing personal data.

# 9 Access and Security

9.1 All partner organisations are required to maintain policies governing levels of access and security and ensure they are adhered to. These policies should be made available to other partner organisations on request.

9.2 Staff must only have access to the information on a need-to-know basis, in order to perform their duties in accordance with one or more of the defined purposes.

9.3 All partner organisations are required to ensure they have in place the organisational and technical measures to enable them to address the issues of physical security, access control, IT security, data protection and confidentiality awareness training, and general levels of security management which are appropriate for their organisation, taking into account the volumes and sensitivity of the personal data which they process. Details of these should be made available to other partner organisations on request.

9.4 Information that has been shared with an organisation should be securely destroyed when no longer needed or in line with organisational guidance.

9.5 Information which is shared between partner organisations should always be transferred using appropriate levels of data encryption. If this is accomplished by email then the transmission must use a method which meets the security standards of both partner organisations.

9.6 It is the responsibility of the providing organisation to ensure that the transmission method has been agreed with the receiving organisation and that they have the correct contact details for the intended recipient within the receiving organisation. Any exchange of information must be part of an agreed process. This means that both those sending and receiving the information should know, before the transfer occurs:

* What is to be sent (quantity, subject matter and format),
* When it is to be sent
* The correct address/contact details for the named recipient
* The purpose and how the information will be treated.
* The method by which it will be transferred

9.7 The receiving organisation should ensure that the individual recipient may only access the Information from a secure device which is password protected, and that unattended devices on which the Information sits must be securely locked to ensure that Information is protected in the event of the device being lost or stolen.

# 10 Indemnity Agreement

Each Party will indemnify the other against any and all costs, expenses, claims and liabilities arising out of any breach of this Agreement by the breaching party and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the breaching party or its sub-contractors, employees, agents or any other person within the control of the breaching party of any data in its possession pursuant to this Agreement.

# 11 Development, Monitoring and Review

11.1 This Agreement will be reviewed regularly (no less than once annually) and will be amended to ensure that it continues to meet the needs and obligations of the Partner Organisations.

11.2 Any partner may request changes to this Agreement, however these will not be approved without agreement from all organisations.

# 12 List of Partner Agencies and nominated staff

The Agreement must be signed by the Senior Information Risk Owner, Data protection Officer or a similar senior authorised representative from each organisation in the partnership.

**Signatories**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Agency** | **DPA Registration Number** | **Executive Member** | **Signature** | **Date** | **Nominated Contact** |
| Plymouth City Council | Z7262171 |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Appendix A: Protection of Information within this agreement.

|  |  |
| --- | --- |
| **Sharing & Destruction Methods** | **Security Requirements** |
| Internal email | Ensure procedures are in place to ensure personal data is not sent to wrong email address.  No personal data to be put into in subject title or sensitive personal data in body of email. |
| Email between partner organisations | Information is only to be emailed between partners using accredited secure email service, provided by either partner.  Ensure procedures are in place to ensure personal data is not sent to wrong email address.  No personal data to be put into in subject title, or sensitive personal data in body of email. |
| Storage of data on mobile equipment / storage. | Any mobile equipment used to store or process this equipment must be owned and managed by the partner and encrypted using accredited encryption solution.  No personal or sensitive information from any of the organisations subject to this Information Sharing Agreement is to be loaded onto personally owned removable media, or any other mobile data storage solution, including personal smartphones. |
| Electronic storage of information | The data within this Information Sharing agreement must be stored on a managed data storage network, which has full access control applied to ensure only authorised people can access the information.  The data storage network must be security accredited annually. |
| Vetting/clearance of staff | All people who will receive and access the personal / sensitive information in this agreement are to be vetted to Baseline Personnel Security Standards. |
| Other communication methods | The information in this agreement can be communicated over the telephone, both fixed line and mobile, as long as unauthorised people cannot overhear details of the information being communicated.  The information in this agreement should not be sent by fax unless there is no alternative. All faxes must use best practice for ensuring the security of faxes. |
| Storage of papers | Protected by one barrier, e.g. a locked container within a secure building/room. Locked filing cabinet for storage if home working. |
| Movement of information within organisation via internal mail | In a sealed envelope with protective marking shown. |
| Movement of information between partner agencies | By post or courier in a sealed envelope using registered mail or equivalent. |
| Movement of information between workplace and home / mobile office | On encrypted memory stick or lockable briefcase for paper documents. Locked filing cabinet for paper document storage if stored off site. |

**Appendix B: Glossary of Terms Used in this Agreement**

**Anonymised information –** information from which no individual can be identified

**Data -** any information, whether in digital or paper format, which is held in a filing system

**Data Controller -** a person who (either alone or jointly or in common with another person) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

**Data processor -** any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Data Protection Act 2018 (DPA)** – the main UK legislation which governs the handling and protection of information relating to living people.

**Data sharing** – the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.

**Data sharing Agreements/protocols** – set out a common set of rules to be adopted by the various organisations involved in a data sharing operation.

**Personal data** – data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

**Data Protection impact assessment (DPIA)** – is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

**Processing of data** – 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, including—

* organisation, adaptation or alteration of the information or data,
* retrieval, consultation or use of the information or data,
* disclosure of the information or data by transmission, dissemination or otherwise making available, or
* alignment, combination, blocking, erasure or destruction of the
* information or data.

**Pseudonymisation Information -** is the process of disguising individual identity. In contrast to fully anonymised data, pseudonymisation allows future or additional data to be linked to the current data, whereby the identity of the patient remains undisclosed. Key-coded data is an example of pseudonymisation.

**Sensitive personal data** – personal data consisting of information as to—

* Racial or ethnic origin
* Political opinions
* Religious or philosophical beliefs
* Trade union membership
* Genetic data for the purpose of uniquely identifying a natural person
* Biometric data for the purpose of uniquely identifying a natural person
* Health data
* Data concerning a natural person's sex life or sexual orientation

**Data Subject Rights** – established by legislation and each organisation is responsible for cooperating with other relevant organisations to implement these rights, which include:

* The right to be informed via Privacy Notices.
* The right of access to any personal information the council holds about a data subject.
* The right of rectification, inaccurate or incomplete data must be corrected within one month.
* The right to erasure.
  + A data subject has the right to have their personal data erased and to prevent processing unless there is a legal obligation to process their personal information.
* The right to restrict processing.
  + A data subject has the right to suppress processing. Just enough information can be retained about them to ensure that the restriction is respected in future.
* The right to data portability.
  + A data subject can be provided with their personal data in a structured, commonly used, machine readable form when asked, if certain legal conditions exist.
* The right to object.
  + A data subject can object to their personal data being used for profiling, direct marketing or research purposes.
* The rights in relation to automated decision making and profiling, to reduce the risk that a potentially damaging decision is taken without human intervention.

**Appendix C: Template tier 2 agreement**

**1 Introduction**

This Information Sharing Agreement provides a commitment by the signatories to ensure that a framework is in place that facilitates the sharing of information between partners and respects the individual’s right to privacy. Information sharing is increasingly important in the provision of services to our communities.

2 Information sharing agreement Purpose

This information sharing agreement facilitates the sharing of information for the purposes set out below.

|  |
| --- |
| We need to share this information because |
| You should explain why sharing this information will help each of the signatories to provide better services to our service users and communities. |
| **Specifically information is shared to achieve:** |
| What is expected to be delivered because of the sharing of this information. |

3 Information being shared

This Information sharing agreement covers the following information, set out in the table below.

|  |
| --- |
| Information to be shared |
| List of all the information being shared. |

**4 Access to the information**

|  |
| --- |
| Who will have access to this information |
| Named people, Job roles or departments |

5 Legal Basis

Information must be shared lawfully. The Data Protection Act provides a legal basis for the processing of personal data which ensures information is disclosed fairly and lawfully. Other specific Acts will allow for this information to be shared.

|  |
| --- |
| Applicable Legislation |
| You need to remember that some information is protected from sharing or disclosure by legislation or Home Office guidance (certain health information, convictions) so you need to make sure that no such restrictions apply to the information you want to share.  The legislation entered here should be the specific legislation relevant to the work that is being undertaken, for example in the case of Social care it would be the care act, if relating to a specific crime, it should be that particular act. All other service specific legislation should be entered, which relates to this piece of work.  The legislation that should not be entered here is the Data Protection Act or other legislation which protects the information, as this is covered further down the document. |

5.1 Data Protection Act Principles

The 6 principles of the Data Protection Act must be met in this Information Sharing agreement. The table below identifies how the 6 principles will be met by both parties subject to this agreement. Please see the Data Protection Act 2018 for the full wording of the principles. The Parties will ensure this Agreement and the manner in which information is shared adheres in all respects to these principles.

|  |  |  |
| --- | --- | --- |
| These are all 6 Principles of the Act. | | This is how they will be met. |
| **1** | Processed fairly, lawfully and in a transparent manner | Please insert how this will be met. Examples include:   * Whether there is a legal basis for processing * Has the data subject been informed who has the information * Is a privacy notice available   Who has been given access to the information |
| **2** | Collected for specified, explicit and legitimate purposes and not further processed for other purposes | Please insert how this will be met. Examples include:   * The purpose the information will be used by each organisation   Whether the information is shared elsewhere & if so, what precautions have been taken. |
| **3** | Adequate, relevant and limited to what is necessary in relation to the purposes | Please insert how this will be met. Examples include:   * How the information will be limited to what is stated in this agreement * Whether information is merged with any other   Whether additional information is collected, and is so what it is used for |
| **4** | Accurate and up to date | Please insert how this will be met. Examples include:   * How information is checked. * How inaccuracies are corrected or updated and when   Who is told about changes |
| **5** | Kept no longer than necessary | Please insert how this will be met. Examples include:   * The retention that is applied   How information is disposed of |
| **6** | Appropriate Security Measures | Please insert how this will be met. Examples include:   * Hard copies stored securely * How electronic copies are secured folder on local computer drive.   How Computer is security patched and virus protected |

5.2 Special Categories of Data

Any information shared as part of this agreement, which is classed as Special Categories of Data is subject to schedule 1 of the Data Protection Act. Additional safeguards need to be applied to meet Part 4 of Schedule 1.

|  |  |  |
| --- | --- | --- |
| These are requirements which apply to satisfy Schedule 1: | | |
| **1** | Employment, social security and social protection | Please delete as necessary. |
| **2** | Health and social care | Please delete as necessary. |
| **3** | Public health | Please delete as necessary. |
| **4** | Archiving, research and statistics | Please delete as necessary. |
| **5** | Substantial public interest | Please delete as necessary, or specify which public interest criteria is met. |
| **6** | Conditions relating to criminal convictions | Please delete as necessary, or specify which public interest criteria is met. |

5.2.1 Additional safeguards for Special categories of Data

|  |  |  |
| --- | --- | --- |
| Additional safeguards which apply to satisfy Schedule 1 Part 4: | | |
| **1** | Appropriate policy document | Please specify how this will be met public interest criteria is met. |
| **2** | Record of processing | Which condition is relied on,  (b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing) |

The Parties will ensure this Agreement and the manner in which information is shared adheres in all respects to the principles of the Data Protection Act

No information will be forwarded on to a third party or sub-contractor without the express written permission of the Data Controller of the disclosing party.

Each party hereby undertakes to apply the security measures recommended or detailed in Appendix A to all information it processes under this Agreement.

6 Information requests

Requests may be received under the Data Protection Act, the Freedom of Information Act 2000 or the Environmental Information Regulations. When a request for information which has been shared under this Information Sharing Agreement is received, the party which receives the request will inform the other and request its views about the disclosure or otherwise of the information.

7 Information retention

The information covered by this agreement will be stored for an agreed time. This retention period is set out in the table below.

|  |  |  |
| --- | --- | --- |
| Organisation name | Period Information retained | Disposal Date |
| Data Processor | Retention period | Date for Disposal |

7.1 Information Disposal

All information subject to this agreement must be disposed of securely at the end of the retention period. Electronic forms of the information must be disposed of securely using a security accredited method of deletion. This includes any copies of the data which has been backed up or copied off site.

All paper forms of the information must be securely shredded. The costs of disposal will be met by the data processor.

8 Agreement Compliance

It is the duty of each party to this Information Sharing Agreement to ensure compliance with this Agreement within their respective organisations.

9 Agreement Breaches

If any information which is shared under this Agreement is lost, stolen, or disclosed to anyone who should not have had access to it, this shall be a breach of this Agreement. The Data Controller for the breaching party must notify the other party of any breach by the breaching party as soon as it becomes aware of the breach. If there is suspicion of a breach, this also must be notified immediately. Investigation into the breach will be conducted by the Data Controller for the breaching party, with relevant escalation.

10 Partners/signatories

The following partners are subject to this data sharing agreement, with the responsible signatory identified, who will sign this Information Sharing Agreement at the end of the document.

|  |  |
| --- | --- |
| Partner | Signatory |
| Partner name |  |
| Partner name |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |