

## DATA PROCESSING AGREEMENT

Between

**Shropshire Council ('The Council')**

and

**[Full name of company] ('Data Processor')**

### **Compliance with the Data Protection Act 2018**

Section 59 of the Data Protection Act 2018 places obligations upon a Data Controller to make sure that any Data Processor it engages provides sufficient assurances that the processing of the data carried out on its behalf is secure. In practice this means that the data processor engaged must provide sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out and must take reasonable steps to ensure compliance with those measures.

This Agreement exists to make sure that both the Data Controller and Data Processor comply with the eight Data Protection Principles contained in the Act and all other terms within the Act.

Under the terms of an agreement between The Council and the Data Processor dated [date], the Data Processor provides [describe the services] which will involve the processing of personal data that are under the Council's control. The processor agrees to act only on the Council's instructions in respect of the data unless Union or Member State law to which the processor is subject, determines otherwise. The personal data to be transferred under this Agreement is as follows:

**[Describe personal data to be transferred – this includes IP addresses and location data including cookies]**

The law does not permit the Council to allow the Data Processor to process this personal data unless the Council complies, and can demonstrate that the Council complies, with certain requirements as set out in the Data Protection Act and the upcoming GDPR. Therefore, this agreement is in place in order to make sure that the Council and the Data Processor discharge their respective obligations.

**Purpose of information sharing**

*State clearly what the purpose of the information sharing is and why the sharing of personal information is required to meet the purpose.*

**Basis for information sharing**

*Outline the basis for sharing including relevant statutory powers, processing conditions and fairness.*

Any sharing of personal information must comply with the fair processing conditions outlined in Article 6 of the GDPR (personal data) and Article 9 (special categories of data).

The key legislation underpinning the data sharing agreement can be found in the Acts below: *Add below a list of the relevant legislation*

**1. Privacy Impact Assessment**

Under the new EU General Data Protection Regulations a Privacy Impact Assessment (PIA), which is an assessment made prior to processing of the impact of the processing on the protection of personal data, will be mandatory in certain circumstances. This will be the case where when taking into account the nature, scope, context and purposes of the processing, it is likely to result in a high risk to the rights and freedoms of individuals. Therefore the data processor will ensure in these circumstances that they complete a privacy impact assessment so that they can assess the risks to individuals and take steps to mitigate against those risks.

**2 Security**

2.1 The Data Processor will take appropriate technical and organisational measures against unlawful and unauthorised processing of the personal data and against accidental loss, destruction of and damage to the personal data. In particular, the Data Processor is required to make sure that they have procedures in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport
- deter deliberate compromise or opportunist attack
- dispose of or destroy the data in a way that makes reconstruction unlikely
- promote discretion to avoid unauthorised access.
- Be ready and prepared to respond to any breach of security swiftly and effectively and all parties must ensure that any breaches are reported to the data controller within one working day.
- Set a deadline for reporting a breach to the relevant data controller
- Maintain a record of personal data and processing activities regarding the data.
- The data processor must ensure that access to information subject to this agreement will only be granted to those professionals who 'need to know' to effectively discharge their duties.
- The data processor will have policies and systems in place to ensure information held on its information systems is held securely and in compliance with industry security standards and legislation

### **3 Personnel**

- 3.1 The Data Processor shall make sure that sufficient processes are in place to check the reliability of all its personnel (whether employees or contractors) that may have access to the personal data and to make sure that they are adequately trained in their responsibilities under the Act and in good handling of personal data. They shall also ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### **4 Purposes**

- 4.1 The Data Processor will act only in accordance with the Council's instructions in relation to the personal data and will not use the personal data for any purpose other than to provide the services under this Agreement. The purpose(s) for which the Data Processor may use the personal data are as follows:

**[Describe purpose(s)]**

The data should not be used for any other purpose that is incompatible with the original purpose/s stated above.

### **5 Adequacy and accuracy**

- 5.1 The data processor will ensure that they will only process personal data they need for the required purpose/s and ensure that any personal data they process and hold is kept up to date and accurate.

## **6 Subcontractors**

- 6.1 The Data Processor is not permitted to subcontract any activity that will involve a third party processing the personal data without the Council's prior written consent.

## **7 Transferring personal data outside the European Economic Area**

- 7.1 The Data Processor will not transfer or permit the transfer of personal data to any territory outside the European Economic Area without the Council's prior written consent.

## **8 Liability**

Under the Data Protection Act 2018 data subjects will be able to take action against both data controllers and data processors and potentially claim damages where they have suffered material or immaterial damage as a result of an infringement of obligations under the DPA ("Compensation"). Under the DPA the Information Commissioner's Office can also fine a data processor or a data controller in relation to any breaches of the DPA.

In the event that the Data Controller or the Data Processor (for the purposes of this clause: "Party A") is ordered by a Court/Tribunal to pay Compensation to a Data Subject or is required to pay a fine by the Information Commissioner's Office, to the extent that such Compensation has arisen as a result of the act, negligence, omission or default of the other party ("Party B"), Party B shall indemnify Party A in respect of that element of the Compensation..

## **9. Rights of the data subject**

### **9.1 Right of access**

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

Individuals have the right to obtain the following from you:

- confirmation that you are processing their personal data;
- a copy of their personal data; and

- other supplementary information – this largely corresponds to the information that you should provide in a privacy notice (see ‘Supplementary information’ below).

If the right is successfully engaged the data controller will confirm in writing and ensure that the data is deleted within one month of the request. The data processors will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

## 9.2 **Right to rectification**

Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the GDPR (Article 5(1)(d)). However, although you may have already taken steps to ensure that the personal data was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

If the right is successfully engaged the data controller will confirm in writing and ensure that the data is deleted within one month of the request. The data processors will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

## 9.3 **Right to restrict processing**

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual’s personal data indefinitely, but will need to have the restriction in place for a certain period of time.

If the right is successfully engaged the data controller will confirm in writing and ensure that the data is deleted within one month of the request. The data processors will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

## 9.4 **Right to object**

Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data.

The right to object only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing.

Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in you; or
- your legitimate interests (or those of a third party).
- In these circumstances the right to object is not absolute.

If you are processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

If the right is successfully engaged the data controller will confirm in writing and ensure that the data is deleted within one month of the request. The data processors will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

## 9.5 **Right to have data transferred**

Under the DPA an individual has the right to have their personal data transferred where:

- personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

In response to such a request the parties will provide personal data in a structured, machine readable format. The information will be provided free of charge within one month of the request by the controller and any processors subject to this agreement must comply with any instructions from the controller that will assist them in complying with such requests.

## 10 **Providing assistance**

- 10.1 The Data Processor will assist the Council promptly with all subject access requests which may be received from individuals whose personal data the Data Processor processes or may have cause to process on behalf of the Council. In order to ensure that the Data Processor can comply with this they must ensure that they have effective record management processes and policies in place.

The Data Processor will ensure that they refer any statutory requests to the Data Controller within 2 working days.

- 10.2 The Data Processor will promptly amend, transfer or delete any personal data that the Data Processor processes or may have cause to process on behalf of the Council, when instructed to do so.
- 10.3 The Data Processor will notify the Council immediately of all communications the Data Processor receives from any person relating to actual or perceived non-compliance with the Act. The Council reserves the right to make the decision to investigate any notified breaches.
- 10.4 The Data Processor will provide the Council with a copy of the personal data the subject of the communication within 7 working days.
- 10.5 The Data Processor will immediately inform the Council of any other breach or suspected breach of the Act involving the Council's personal data.

## **11 Audit**

- 11.1 The Data Processor will permit the Council to monitor compliance with the terms of this Agreement, which may involve the Council or its nominated representative visiting and accessing any premises where the personal data are being processed without notice.

## **12 Termination of the Agreement**

- 12.1 This Agreement shall cease to be in force immediately upon termination or expiry of the Data Processor's obligations in relation to the Services. On termination of this Agreement the Data Processor shall, within 30 days, securely deliver to the Council or destroy, at the Council's sole option, all the Council's Data in its possession or under its control and in non-proprietary file formats that can be read by readily available office productivity software.
- 12.2 The Data Processor is required to provide a certificate of destruction within 7 working days.
- 12.3 The Council shall be entitled to terminate this Agreement forthwith by notice in writing to the Data Processor if:-

1. the Data Processor commits a material or persistent breach of this Agreement which, in the case of a breach capable of remedy, shall not have been remedied within fourteen (14) days from the date of receipt by the Data Processor of a notice from the Council identifying the breach and requiring its remedy; or
2. the Data Processor becomes insolvent, has a receiver, administrator, or administrative receiver appointed over the whole or any part of its assets, enters into any compound with creditors, or has an order made or resolution passed for it to be wound up (otherwise than in furtherance of a scheme for solvent amalgamation or reconstruction).

### **13 Transferring this arrangement**

- 13.1 This arrangement is personal to the Data Processor and may not be assigned, nor have any of the rights or obligations contained within it transferred without the Council's written consent.

### **14 Data Retention Policy**

- 14.1 The Data Processor shall comply with the Data Retention Guidelines as issued by the Council and amended from time to time. This may require certain data to be identified for retention and made available to the Council in electronic form by the Data Processor. The Data Processor will also only retain data for as long as is necessary for the relevant purpose/s and be securely deleted when no longer needed unless there is a legal requirement to keep the data for longer.

### **15 Indemnity**

- 15.1 The Data Processor agrees to indemnify the Data Controller against any loss, damages, costs, compensation, fines, penalty or awards made against the Data Controller as a result of the Data Processor's breach of the Agreement.

### **16 Law**

- 16.1 This agreement is governed by and will be interpreted in accordance with English law. In the event of a dispute between the parties, it is agreed that the English courts will have exclusive jurisdiction to hear the case.

### **17 Third party rights**

- 17.1 The Council and the Data Processor are entering into this Agreement for the benefit of the parties and the individuals whose personal data the Data Processor will process, each of whom will be entitled to enforce it. Other than that, no other person will have any enforceable rights under this Agreement and the Contracts (Rights of Third Parties) Act 1999 will not apply.



**18. IP addresses and cookies**

18.1 Under the DPA IP addresses and cookie tracking will be considered as personal data as they are classed as online identifiers in some cases. Therefore if the processing involves this type of data the obligations imposed on the processor will also apply to this data.

Signed for and on behalf of the Data Processor:

Signature: .....

Print name: .....

Position: .....

Date: .....