

Information Sharing Agreement

Between

**Shropshire Council
(for the Shropshire Hills AONB Partnership team)**

and

Shropshire Hills AONB Trust

Version 2.0

Document owner	Phil Holden, AONB Partnership Manager
Document author and enquiry point	Phil Holden, AONB Partnership Manager
Document authoriser	Phil Holden, AONB Partnership Manager
Date of document	12 August 2022
Version	2.0
Document classification	none
Document distribution	Chair, Secretary and Treasurer of the Shropshire Hills AONB Trust
Document retention period	Until date of next review
Next document review date	12 th August 2023

Contents

1. List of Partners to the Agreement
2. Information to be shared
3. Purpose of Information sharing
4. Basis for information sharing
5. Exchange of information
6. Terms of use of the information
7. Data quality assurance
8. Data retention, review and disposal
9. Access and security
10. General Operational Guidance/process
11. Privacy Impact Assessment
12. Liability
13. Rights of the data subject
14. Management of the Agreement
15. Version History
16. Signatories

Appendix A - Definitions

1. List of Partners to the Agreement

This is a data sharing agreement between Shropshire Council (on behalf of the Shropshire Hills AONB Partnership) and the Shropshire Hills AONB Trust, relating to the sharing of personal information.

The partners are **Joint Controllers** of data in relation to this agreement. The Data Controllers within each organisation are:

- Phil Holden, AONB Partnership Manager (employed by Shropshire Council)
- Chair & Treasurer of the Shropshire Hills AONB Trust

It will be the responsibility of each party to:

- Have realistic expectations on information sharing
- Maintain standards in respect of information sharing
- Have processes in place to control the flow of information
- Meet Data Protection Act 2018 requirements

2. Information to be shared

The data that will be shared between the parties is the names, addresses, email addresses, telephone numbers and bank/building society details (as necessary) of:

- Friends of the Shropshire Hills AONB
- Business Supporters
- AONB Conservation Fund grant applicants and recipients
- Donors and participants in other programmes of the Trust.

No relationship data will be stored or exchanged.

3. Purpose of Information sharing

The data is being shared to enable both the AONB Partnership and AONB Trust to work effectively together

- to administer the joint Friends of the Shropshire Hills AONB scheme
- to administer the Trust's Business Supporters Scheme
- to administer grant applications and awards through the AONB Conservation Fund
- to receive donations and operate specific appeals.

4. Basis for information sharing

The sharing of information is done on the legal basis of the legitimate interests of the data subjects and of the Shropshire Hills AONB Partnership and the Shropshire Hills AONB Trust. The data which is held and shared is the minimum which is necessary to operate the programmes and schemes concerned.

The Shropshire Hills AONB Partnership's privacy policy can be viewed at <https://www.shropshirehillsaonb.co.uk/privacy-policy>

The Shropshire Hills AONB Trust's privacy policy can be viewed at <https://www.shropshirehillsaonb.co.uk/help-to-look-after/shropshire-hills-aonb-trust>.

Any sharing of personal information must comply with the fair processing conditions outlined in Article 6 of the GDPR (personal Information) and Article 9 (special categories of personal data) and Schedule 9 of the Data Protection Act 2018 (personal information) and Schedule 8 or Schedule 1, Part 2 (special categories of personal data).

5. Exchange of information

Documents not containing personal or commercially sensitive data can be shared by whatever is considered to be an appropriate medium by the partners.

Documents containing personal data or commercially sensitive data will only be shared by secure methods;

- Web portals with industry standard security and authenticated access (external Sharepoint site)
- Secure email solutions with industry standard security e.g. Egress
- Encrypted files with industry standard security
- Confirmed delivery post

6. Terms of use of the information

Information will only be used for the specified purpose, to enable both organisations to work effectively together to support the specified programmes.

Where it is reasonably determined that further information is necessary to fulfil statutory duties and/or other requirements this Agreement will be reviewed in full or in part as appropriate.

Whenever possible data shared, should be anonymised, unless requested at personal level.

Information on children/young people will be shared with industry standard security.

Both parties will store "person identifiable" data shared between both partners on secure systems which can only be accessed by a restricted number of appropriate staff with appropriate security safeguards.

Both parties will use the data supplied for the purposes stated and will not pass such data to third party organisations outside the remit of specified partners in agreement without prior written consent.

It is also prohibited under this agreement for sub-processors to be used without the prior consent of the Data Controller.

Both parties will comply with their obligations under the Freedom of Information Act 2000 and may consult with the other party if necessary if requests relate to information shared but will remain responsible for responding to the request.

7. Data quality assurance

Information shared will be adequate, relevant, accurate and up to date.

Both parties to this agreement will adhere to their internal data quality policies and procedures when storing, sharing and updating information.

Information discovered to be inaccurate, out-of-date or inadequate for the purpose should be notified to the relevant Data Controller within 2 working days. The Data Controller will be responsible for correcting the data and notifying all other recipients of the information who must also make sure the correction is made.

8. Data retention, review and disposal

Electronic and paper records will be retained and disposed according to published record retention and disposal policies of both parties, these policies should be based on The Records Management Standards Society guidance.

Any paper records held by any of the parties that contain personal data reasons should be destroyed using file shredding hardware, in accordance with statutory retention periods.

The working relationship with the Shropshire Hills AONB Trust is an ongoing partnership. This information Sharing Agreement is being put in place for 3 years, and will be reviewed on 12 August 2025. If a further Agreement is not put in place at that time, data which has been shared which is not available in the public domain will be destroyed.

9. Access and security

Both parties will each comply with their obligations under the Data Protection Act 2018 and will not breach their common law duty of confidentiality.

Each party will make sure they take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In particular, each party must make sure 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 ICO or the Controller where required.
- Maintain a record of personal data and processing activities regarding the data.

Access to information subject to this agreement will only be granted to those professionals who 'need to know' to effectively discharge their duties.

All Shropshire Council and staff from all other parties to this agreement must comply with Council data protection and confidentiality policies as part of their employment contract.

Shropshire Council and all other parties to the agreement 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.

10. General Operational Guidance/process

Appropriate technical and organisational processes are in place to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

All parties to the agreement will ensure adequate resources are available to extract and securely transfer accurate, timely and complete data electronically.

11. Data Protection Impact Assessment

Under the UK General Data Protection Regulation a Data Protection Impact Assessment (DPIA), 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. <https://ico.org.uk/for-organisations/guide-to-data->

protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ . All controllers subject to this agreement must complete a DPIA where required.

12. Liability

Under the Data Protection Act (DPA) 2018 the 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.

13. Rights of the data subject

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. Any data processors will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

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. Any data processors will

comply with any instructions in regards to the personal data in such circumstances within 5 working days.

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. Any data processors will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

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. Any data processors will comply with any instructions in regards to the personal data in such circumstances within 5 working days.

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.

14. Management of the Agreement

Any complaints or breaches of the agreement will be dealt with by the relevant controller of the data.

This agreement will be reviewed on an annual basis.

All complaints or breaches relative to this agreement will be notified to the designated Data Protection Officer of the relevant organisation in accordance with their respective policy and procedures.

Each party will make sure that all breaches of agreement, internal discipline, security incidents or malfunctions will be managed in accordance with their own local policies and procedures to ensure compliance with the Data Protection Act 2018.

Both parties to this Agreement will undertake to indemnify the other against any legal action arising from any breach of this Agreement by any person working for or on behalf of its own organisation.

The data may only be shared with the parties to this agreement and will not be shared with any other third party or any other Authority without the explicit written consent of the Data Controller.

Any party who receives a request for information under the subject access provisions of the Data Protection Act 2018 or Freedom of Information Act 2000, must progress it in accordance with its own internal procedures.

However, it is expected that Officers in the originating organisation will liaise with Officers in the partner organisation as necessary to agree on relevant exemptions from disclosure.

The Information Sharing Agreement will cover the period 12th August 2022 to 11th August 2025. It will be reviewed by 12th August 2023 and every 12 months thereafter.

Any partner organisation can suspend the Information Sharing Agreement for 30 days, if they feel that security has been seriously breached.

Notification of termination and/or completion by either party must be given in writing with at least 30 days' notice.

The following officers will have responsibility for carrying out the obligations in this Agreement on behalf of the parties and are the initial point of contact for any queries relating to this Agreement or the information shared under it.

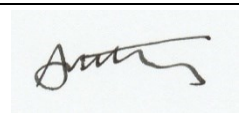
On behalf of Shropshire Hills AONB Trust	
Name of officer	Anthony Morgan
Position	Chair, Shropshire Hills AONB Trust
Telephone number	01547 530342
Email	agmorgan100@btinternet.com


On behalf of Shropshire Council	
Name of officer	Phil Holden
Position	AONB Partnership Manager
Telephone number	01743 254741
Email	phil.holden@shropshire.gov.uk

15. Version History

Date issued	Version	Status	Reason for change
8 December 2021	1.0	Draft	n/a
12 th August 2022	2.0	Final	completion

16. Signatories

Authorised signatory for and on behalf of Shropshire Hills AONB Trust	
Print name	Anthony Morgan
Position	Chair
Date	17 th August 2022

Authorised signatory for and on behalf of Shropshire Council	
Print name	Phil Holden
Position	AONB Partnership Manager
Date	17 th August 2022

Appendix A Definitions

Personal Data

Data which relates to a living individual who can be identified;

- a) from those data, or
- b) 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.

It should also be noted that the definition of personal data is extended to include IP addresses.

Sensitive or Special Categories of Personal Data

Sensitive or Special Categories of Personal Data means personal data consisting of;

- a) racial or ethnic origin of the data subject
- b) political opinions
- c) religious beliefs of other similar beliefs
- d) trade union membership
- e) physical or mental health
- f) sexual life
- g) commission of alleged commission of offences
- h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
- f) Genetics
- g) Biometrics (where used for ID purposes)

Data subject - means an individual who is the subject of personal data.

Data Controller – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

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

Processing – 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, adaption 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