1. **Parties**

This Information Sharing Agreement (ISA) defines the arrangements for processing data and information between:

1.1 **Oxford Brookes University (OBU)** Please tick as applicable (see Appendix A):

Headington Campus Data Processor

OX3 0BP, Oxford, UK Data controller

1.2 The party/parties whose details are set out in the table below :

|  |  |
| --- | --- |
| Please tick as applicable (see Appendix A): Data ProcessorData Controller | |
| Name: |  |
| Address: |  |

1. **Single point of contact (SPoC)**  i.e who will handle the data sharing (see Appendix A):

|  |  |
| --- | --- |
| **OBU** | **Party/Parties under Section 1.2** |
|  |  |

1. **Purpose of the data sharing** i.e. why is the information being shared (see Appendix A):

|  |
| --- |
|  |

1. **Data items to be shared** i.e. what information is being shared (see Appendix A):

|  |
| --- |
|  |

1. **Basis for sharing, consent and privacy notice** i.e what is the legal justification for sharing/ has consent been gained if required and by what means/ has a privacy notice been issued (see Appendix A):

|  |
| --- |
|  |

1. **Secure methods of data sharing** i.e. how will the information be shared (see Appendix A):

|  |
| --- |
|  |

1. **Secure data storage** i.e. how will the information be stored (see Appendix A):

|  |
| --- |
|  |

1. **Data retention and disposal** i.e how long will the information be kept and how will it be destroyed (see Appendix A):

|  |
| --- |
|  |

1. **SAR, FOI requests and Security Incident procedure** i.e who to contact if applicable (see Appendix A):

|  |  |
| --- | --- |
| **OBU** | **Party/Parties under Section 1.2** |
| Information Compliance team  Email: [info.sec@brookes.ac.uk](mailto:info.sec@brookes.ac.uk)  Phone: 01865-484354 |  |
| Pre-defined inclusions/exclusions: | |

1. **Timescale for DSA review** i.e. when will the effectiveness of the DSA be assessed (see Appendix A):

|  |
| --- |
|  |

*This agreement must be formally approved and signed by all parties under Section 1 and a member of the Information Compliance team at Oxford Brookes University before any data sharing takes place. All parties will ensure that the Data Sharing Agreement and any associated documents are known and understood by all staff involved in the process.*

|  |  |  |  |
| --- | --- | --- | --- |
| **On behalf of Oxford Brookes University:** | | **On behalf of** | |
| Name |  | Name |  |
| Job Title |  | Job Title |  |
| Date |  | Date |  |
| Signature |  | Signature |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **On behalf of the Information Management Team at Oxford Brookes University:** | | | |
| Name |  | Signature |  |
| Date |  |

**Appendix A** **Notes to completing the Information Sharing Agreement**

**Note to Section 1. Parties and Section 2. Single point of contact (SPOC)**

The agreement should clearly identify all the parties that will be involved in the data sharing and should identify a person or department serving as the coordinator of the data sharing. It should also specify whether each party acts as a data controller or as a data processor in respect of the processing. This is particularly important in situations such as a data breach where it will be necessary to determine which organisation has data protection responsibility.

A Data Controller decides:

* to collect the personal data in the first place and the legal basis for doing so
* which items of personal data to collect, ie the content of the data
* the purpose or purposes the data are to be used for
* which individuals to collect data about
* whether to disclose the data, and if so, who to
* whether subject access and other individuals’ rights apply ie the application of exemptions
* how long to retain the data or whether to make non-routine amendments to the data

A Data Processor may decide:

* what IT systems or other methods to use to collect personal data
* how to store the personal data; the detail of the security surrounding the personal data
* the means used to transfer the personal data from one organisation to another
* he means used to retrieve personal data about certain individuals
* the method for ensuring a retention schedule is adhered to
* the means used to delete or dispose of the data

**Note to Section 3. Purpose of the data sharing**

The agreement should explain why the data sharing is necessary, its specific aims and benefits, either to individuals or to society more widely. This should be documented in precise terms so that there is no misunderstanding as to the purposes for which data may be shared and shared data may be used.

**Note to Section 4. Data items to be shared**

The agreement should explain the types of data that are intended to be shared with the parties stated under Section 1. This may need to be quite detailed, because in some cases it will be appropriate to share certain details about someone, but not other, more sensitive, data in the same document. In some cases it may be appropriate to attach ‘permissions’ to certain data items, so that only certain members of staff, for example ones that have received appropriate training, are allowed to access them.

Where **sensitive** data is to be shared i.e. data containing the racial or ethnic origin of the data subject, his political opinions, his religious beliefs, trade union membership, his physical or mental health condition, his sexual life, or his criminal record, this needs to be clearly stated as additional care will be required.

**Note to Section 5. Basis for sharing, consent and privacy notice**

Clearly explain the legal power which allows sharing. Under the GDPR you must declare one of the following lawful basis to use personal data:

The individual has given consent to the processing of his or her personal data for one or more specific purposes;

We need to use this for the performance of a contract or to enter into one;

It is necessary for compliance with a legal obligation;

To protect the vital interests of persons;

Needed for task carried out in the public interest or exercise of official authority;

Used for the legitimate interests of the data controller.

A **privacy notice** will have to be provided to the individuals whose data will be shared, either at the point of obtaining consent or if this is not applicable by other specified means.

**Note to Section 6. Secure methods of data sharing and Section 7. Secure data storage**

The format of the data to be shared needs to be compatible with the systems used by all parties. Sufficiently secure methods must be used when transferring personal data both electronically and in hard copy form. Where confidential and/or sensitive data is to be send electronically, it is recommended that the data is encrypted to an acceptable standard (i.e. compliant with FIPS 140-2 (cryptographic modules, software and hardware) and FIPS 19) prior to transfer and protectively marked. Encryption passwords must not be relayed using the same communication channel as the data.

All hardcopy data must be posted using the parties’ approved mail delivery company. All confidential and/or sensitive data must be identified and send with the appropriate level of tracking. Personal information must be labelled ‘private and confidential’ and ‘addressee only’ where appropriate.

Sufficiently secure methods must equally be used when storing personal data both electronically and in hard copy form. Data files should only be accessible to the minimum relevant required people and be adequately secured i.e. password protected, securely locked away, limited permissions etc. Extra care should be taken where the data is confidential and/or sensitive.

**Note to Section 8. Data retention and disposal**

The agreement should include a time frame for the retention of the data in line with the parties’ retention schedule (see Appendix C for reference on OBU’s retention schedule). After the appropriate retention time the data should be securely destroyed/ disposed of, the means by which are to be included in the agreement.

**Note to Section 9. SAR, FOI requests and Security Incident procedure**

The agreement should explain what to do when either party receives a Subject Access Request (SAR), or a Freedom of Information (FOI) request for access to shared data and what to do in case of a Security Incident. Firstly should identify a person or department serving as the point of contact for such requests/incidents. Secondly it should give a broad outline of what data will normally be released under a SAR or FOI request and refer to a publication scheme if applicable.

**Note to Section 10. Timescale for DSA review**

Both parties should agree on a timeframe for reviewing the data sharing to establish if the sharing is still required and if the agreement still adequately covers the nature and governance of the data sharing. The agreement should be updated accordingly in case of any changes.

**Appendix B Data Protection (GDPR) Principles**

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
2. collected for specified purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

**Appendix C References**

For OBU policies, procedures and legislation, including the Information Sharing & Transfer Policy and the Information Security Incident Management Policy please visit:

<http://www.brookes.ac.uk/it/information-management/policies-procedures-legislation/>

For OBU’s retention schedule please visit:

<http://www.brookes.ac.uk/it/information-management/records-management/>

For the ICO’s Data Sharing Code of Practice please visit:

<https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf>