
# Aimhigher Database Information Sharing Agreement

**Version 1.1**
**February 2012**

# Information Sharing Agreement for Aimhigher

## 1 Policy Statement and Purpose of this Information Sharing Agreement

1.1 This web enabled database is used to record Aimhigher and institutional Widening Participation activities, their participants, and the learning organisations they attend, as well as other related data. Data will be used to monitor and evaluate the impact of WP activities for under-represented groups.

1.2 The purpose of this Information Sharing Agreement (ISA) is to facilitate the gathering, sharing, processing and publication of data through the Aimhigher Database (from here on in referred to as *the Database* and is located at http://www.aimhigherwm-activities.org/admin/index.asp)

1.3 The Database is of greatest use if all participating partners input the data they have each gathered as part of Aimhigher and institutional Widening Participation activities. A list of participating Partner Organisations (signatories) to this Information Sharing Agreement can be found at Appendix B.

1.4 For the purposes of this agreement, each of the other Partner Organisations will be *Data Controllers (* as defined within the Data Protection Act 1998).

## 2 Summary of Roles and Responsibilities

| Role | Organisations / Partners | Key Responsibilities |
|---|---|---|
| Lead organisation and Lead Data Controller | **Aimhigher Co-ordination team (university of Birmingham)** | Establishment of agreements<br>Ensure all relevant staff are aware of the existence of Aimhigher's Information Sharing Agreement (ISA) and the Aimhigher Information Sharing Protocol (ISP)<br>Monitoring of operation<br>System management, administration, security, data protection, development, maintenance, support, guidance and training<br>Oversight of breaches<br>Annual review |
| Data Controllers | **Higher Education Institutions**[1] seeking database access rights | Sign the ISA and ISP (following consultation with own Data Protection Officers)<br><br>Ensure database users have a Criminal Records Bureau Check: Enhanced Disclosure.<br><br>Ensure database users understand the ISA and ISP, the Data Protection Act and relevant legislation.<br><br>Ensure database users sign the user registration and agreement form (see Appendix E) |

[1] Includes consultants – e.g. Health Care Strand

| | | |
|---|---|---|
| | | Notify the Lead Data Controller of changes to the list of database users as they arise.<br><br>Ensure identifiable participant data is only held on the database when explicit, informed and freely given consent has been provided.<br><br>Adhere to agreement and database user guidance<br><br>Ensure Data Processors (see below) are able to meet their responsibilities |
| Data Processors | University staff nominated by Data Controllers as users of the database. | Be aware of the ISA.<br>Adhere to agreement and database user guidance |

## 3. Legal Basis for Data Exchange

3.1 All data that are gathered, shared, processed and published as part of this agreement will at all times be compliant with applicable legislation

3.2 Data controllers are responsible for ensuring the explicit, informed and freely given consent of all participants, to ensure data are processed fairly and lawfully. Any breaches of this agreement by a Partner Organisation must be reported to the Aimhigher Management Group as soon as it becomes apparent. The Aimhigher Management Group will monitor the progress of partner organisations in resolving such breaches.

3.3 Data controllers will ensure that all relevant staff within the sharing organisations are aware of the existence of Aimhigher's Information Sharing Agreement and the Aimhigher Information Sharing Protocol.

## 4. Data

### 4.1 Input into the shared Database

#### 4.1.1 What data must be input?

- Data to be input electronically will be captured via centrally or locally devised paper documentation that clearly indicates the data required.
- The data fields to be input into the database can be found at Appendix A.

#### 4.1.2 Who is going to be responsible for input and ensuring accuracy?

- Each Data Controller of this agreement is responsible for the input of data gathered as part of their own Aimhigher and institutional Widening Participation activities.
- Each Data Controller will be responsible for the accuracy of the data that they input to the database.
- If a Data Controller uses a third party to input data (data processors), they must ensure that the third party is aware of this Information Sharing Agreement and that terms are passed on in contracts/agreements
- All users of the database will complete a registration and user agreement form before they are granted access.

#### 4.1.3 How will you keep a record of what data has been input?

- Each Data Controller will keep a log of Widening Participation activities that they have initiated and clearly show if the relevant documentation has subsequently been input into the database.

- All documents should be clearly marked as having been input.

4.1.4 **How is this information to be processed and used?**

- Identifiable participant data will be shared between Data Controller directly through the Database or other media provided it is in the context of this Information Sharing Agreement and is done in a secure manner (secure as defined in Principle 7 of the Data Protection Act 1998).
- Data may be shared internally within a Data Controller, for the purpose of monitoring and evaluation only, provided it is done in a secure manner (secure as defined in Principle 7 of the Data Protection Act 1998).
- Personal participant data will be used for WP Aimhigher and institutional monitoring and evaluation purposes (elements will involve matching to other data sets), provision of information and promotion of Aimhigher and institutional activities only. Personal participant data must not be used for other marketing purposes by either the Data Controller or data processors on their behalf.

4.1.5 **Who will have access to this data?**

- Access levels will be used to provide users with appropriate data only
- The data available through each access level is detailed in Appendix C.
- A list of user roles and their access levels is provided in Appendix D.
- User accounts providing access to Personal Data as defined in Appendix A will only be issued to users with a Criminal Records Bureau Check: Enhanced Disclosure.
- The Lead Data Controller will maintain a list of individuals associated with data entry and their access levels and review this annually.
- Data Controllers will notify the Lead Data Controller of changes to the list of individuals as they arise.

4.1.6 **Timescales**

- As well as being accurate data must be input in a timely manner. This will be dependent upon the Data Controllers requirements for local and national reporting.

4.1.7 **How securely does the data need to be stored?**

- Each Data Controller must have internal security documents and procedures that are available for inspection on request by any and all of the Data Controllers.
- Data will be transferred, processed and held in a safe and controlled way by each Data Controller. Access to common personal data will be restricted to identified roles as listed in Appendix D.
- The data will be stored securely on a web-server which will be managed by the Lead Data Controller and accessed through password protected user accounts only. Electronic records of identifiable participant data can only be processed via secure network space.
- The Database will be accessed from a computer at a secure location only.
- Paper copies of records will be retained by the commissioning Data Controller and / or any third party data processors, who will store them securely in appropriate locations.

4.1.8 **How long are you going to keep the data?**

- Retention periods will be proposed by the Lead Data Controller in consultation with Data Controllers. Data Controllers will be notified before routine deletion takes place. Paper copies will be retained in accordance with Data Controllers' individual retention policies.
- At the end of the retention period, electronic data and paper copies will be destroyed using secure disposal methods: in the case of paper records, through shredding, and electronic records, through permanent deletion.

4.1.9 **Further use of data**

- Data can be transferred internally within Data Controllers where necessary

- Personal data originating from one Data Controller may NOT be transferred to a third party by another Data Controller without first gaining the written consent of the originator.

4.1.10 **Subject Access Requests**

Individuals whose personal information is held on the database may request to see the information that is held about them. Requests may also be made for a correction of any personal information which is proven to be inaccurate. Subject Access Requests (SARs) received by Data Controllers will be referred to the Lead Data Controller.

4.2 **Publication of data from the shared Database**

4.2.1 The data stored on the system will be used by signatories to this agreement to support the production of reports for monitoring and evaluation purposes. Data on participants will be aggregated in such a way as to ensure confidentiality. The personal data of individual participants will not be published unless they express consent and agreement has been obtained.

## 5 Review of Information Sharing Agreement

5.1 This Information Sharing Agreement will be reviewed by the Partnership Group in the summer term of each academic year, to enable appropriate amendments to be negotiated and implemented for the next academic year

## 6 Closure / Termination of Agreement

6.1 If a Data Controller wishes to terminate this Information Sharing Agreement it shall serve notice to all other Data Controllers giving at least 30 days notice. Termination will result in data originally provided by the terminating Data Controller being retained by the Project. A copy of this data will be provided to the terminating Data Controller.

# 7 Appropriate Signatories

This agreement is signed and endorsed by an employee of the Data Controller who has the authority to sign on behalf of the Data Controller.

I the undersigned do hereby agree to implement the terms and conditions of this agreement. I confirm that before signing this Information Sharing Agreement I have consulted with DPO (Data Protection Officer) for my organisation.

This agreement is signed on behalf of the Data Controller as follows:

Name of Organisation: _____

Name of Officer: _____

Title: _____

Signature: _____

Date: _____

This agreement is signed by the lead organisation and lead data controller (Aimhigher Co-ordination team)

Name: _____

Signature: _____

Date: _____

# Appendix A - Personal Data (Data Covered by this ISA)

This learner specific data is collected and shared for monitoring purposes to enable medium and long term evaluation, and matching with other data sets. It will be used for the production of statistics. While not inherently personal in nature, some of the data recorded may, if used in conjunction with other recorded details, be used to specifically identify an individual, and should hence be dealt with accordingly.

| **Data** | **Definition** |
|---|---|
| First Name | First name(s) of learner |
| Last Name | Family name of learner |
| Birth date | Date of Birth of learner |
| Address | Full address of the learner in up to 4 fields |
| Area | Name of institution |
| Postcode | Learner's postcode |
| Telephone | Learner's home phone number |
| Mobile | Learner's mobile phone number |
| Gender | Sex/Gender of learner |
| Ethnicity | Ethnic background of learner |
| Disability | Any and all classifications, if any, that would identify the learner as disabled. |
| Did parents study at HE | Whether the learner's parents have under taken education at level 4 or above. |
| Academic Year at Enrolment | The academic year during which the learner was entered onto the system. |
| Looked after | Does the learner have looked after status. |
| In receipt of 16-19 Bursary | In receipt of 16-19 Bursary |
| FSM | Is the learner in receipt of FSM |
| Year Group at Enrolment | The academic year group the learner was studying in at the time of enrolment onto the programme. |
| UCAS number | If the learner has made an application and is known |
| HE course | HE course accepted on |
| Date Completed | When completed HE programme |
| Learner Agreement | Complete for consents |
| Parental/Learners consent participation | |
| Parental learners consent for evaluation study | |
| Name Of Parent/Carer | Name of person with parental responsibility for learner |
| Relationship To Learner | Relationship to learner of person with parental responsibility |
| Parental Occupation | Parent/carer occupation as supplied by the parent. |
| Establishments Attended | Names of learning organisations the learner has attended. |

# Appendix B - List of Partner Organisations (signatories) of this ISA

***Lead Organisation and Lead Data Controller:**
Aimhigher – University of Birmingham

***Data Controllers:**
The University of Birmingham
Birmingham City University
University College Birmingham
Aston University
Jean Knee – consultant Health Care Strand
* as defined within the Data Protection Act 1998

# Appendix C - Guide to Access Levels

This appendix provides details of the access levels used to log-on to the Database and what data can be accessed through a particular access level:

| | | What data can be accessed through this access level? | | |
|---|---|---|---|---|
| **Access Level Name** | **Which types of staff are assigned this access level?** | **Non-personal Learner Data** | **Personal Learner Data** | **Other** |
| External User | Organisations using the school and postcode lookup tools | None | None | None |
| Activities – Area Project Manager | Staff from Data Controllers or Processors responsible for data input to the Database relating to individual projects | Relating to learners from the related institution only | Relating to learners from the related institution only | None |
| Activities - Area Super User | Staff from Data Controllers responsible for localised management of the Database | Relating to learners from all institutions | Relating to learners from all institutions | User account details |
| All access – Super User | Staff from Data Controllers responsible for cross area management of the Database | Relating to learners from all institutions | Relating to learners from all institutions | User account details Can add/amend certain database fields (e.g. lead projects and organisations) |
| All access – Webmaster | Database developers | Relating to learners from all institutions | Relating to learners from all institutions | User account details |

# Appendix D - Database Users

This appendix gives details of the Database users, that is their Organisation, Department, Position/Role and Access Level (Access Levels are defined in Appendix C).

| **Organisation** | **Department** | **Position/Role** | **Access Level** |
|---|---|---|---|
| University of Birmingham | Aimhigher Area Office | Area Coordinator | All access - super user |
| University of Birmingham | Aimhigher Area Office | Evaluation Officer | All access – super user |
| Universities | Outreach | Staff and management | Activities – Area Project Manager |
| Consultant (Health) | NA | Health Care Strand Consultant | Activities – Area Project Manager |
| *Winona eSolutions | Winona eSolutions | Managing Director | All access – Super User |
| *Winona eSolutions | Winona eSolutions | Site Developer | All access – Super User |

*Winona eSolutions are a registered CRB umbrella body through an Arts Council funded project London Schools Arts Service (LONSAS). They are listed on the CRB website www.crb.gov.uk in their umbrella organization database. Through the service they have access to highly confidential material relating to individuals and were thoroughly vetted for suitability as a CRB umbrella body, compliance with which is audited by CRB on an annual basis. In addition Winona is registered with the Information Commissioner's Office for Data Protection (registration no. Z9167559).*

# Appendix E - User Agreement

## Database User Registration and Agreement Form

This agreement is to be signed by all staff who require access to the Aimhigher Database.

All data that is gathered, stored, shared and published will be done so in accordance with the Aimhigher Information Sharing Agreement and the Aimhigher Information Sharing Protocol, Data Protection Act 1998, Human Rights Act 1998 and Freedom of Information Act 2000. Data will be transferred, processed and held in a safe and controlled way. Identifiable participant data will only be held on the database when explicit, informed and freely given consent has been provided. Personal participant data will be used for WP/Aimhigher monitoring and evaluation purposes, provision of information and promotion of Aimhigher activities only. Data will be processed fairly and lawfully.

I the undersigned understand this agreement and do hereby agree to implement the terms and conditions of this agreement.

Organisation: _____

Name of Officer: _____

Job Title: _____

Signature: _____

Date: _____

Email Address: _____

Please note applications for user accounts must only be made if you have an Enhanced Criminal Records Check.

**Ends**