INFORMATION SHARING AGREEMENT BETWEEN

Attendance, Child Employment & Entertainment, Elective Home Education/Children Missing Education (ACE), Westminster City Council (otherwise known as the "Licensing Authority")

And

(Hertfordshire Music Service)

Date of agreement November 2017

For review [October 2018]

Table of contents

Information Sharing Agreement

1. OBJECTIVE OF THE AGREEMENT

- Provide a framework for ACE employees to receive and deliver information for a better service
- Consider the controls required for information sharing
- Ensure that expected standards are met and that partners to information sharing are aware of the obligations of consent.
- Establish a mechanism for the exchange of information between ACE and other organisations.
- All Signatories to this agreement agree to provide appropriate evidence with regard to the processing of personal data held within their respective systems and with regard to their data handling processes.

2. LEGAL BASIS FOR SHARING DATA

- The Data Protection Act 1998
- The Human Rights Act 1998 and the European Convention on Human Rights
- The Children (Performances & Activities) (England) Regulations 2014
- The Children & Young Persons Act 1963
- The Freedom of Information Act 2000
- The Contract of Agreement for a Body of Persons Approval

3. PARTIESTO THE AGREEMENT

The parties participating in this data sharing arrangement and who agree to be covered by this Protocol (as per the Agreement at Appendix A) include:

- The owner of information for any application for a Performance Licence or a Body of Persons Approval [BOPA] is the entertainment performance production body otherwise referred to as the **"Applicant**" – in this instance **Hertfordshire Music Service**.
- The "Applicant" will share information pertaining to a child or children to enable the Licensing Authority – Westminster City Council – to consider and approve a licence or BOPA for the purposes of undertaking an entertainment performance.
- Under its current licencing duties, the Licensing Authority will share relevant information of a licence or BOPA with other local authorities based on where the child is resident.
- Where necessary, the Licensing Authority will share relevant information pertaining a licence/BOPA application with the school the child is registered at.

4 PURPOSE(S) FOR WHICH INFORMATION IS TO BE SHARED

- To enable the Licensing Authority to consider and approve a performance licence or a BOPA as conferred on it by law.
- To enable a child's resident local authority to have access to information pertaining to the participation in performances with WCC of children resident in their borough, so as to enable WCC to fulfil its notification duties as conferred by law.
- Where relevant, to enable local authority with supervision responsibilities over entertainment performances to undertake responsibilities conferred on it by law.

Please Note: Consent is not required in order to disclose information as above.

5. TYPES OF DATA TO BE SHARED

- Names and dates of birth of children
- Addresses of children
- School of children
- Passport photograph of children (in the case of Licence but not BOPA)
- Venue and date of relevant performance

Please Note: Consent is not required to undertake processing of information

6. DATA HANDLING REQUIREMENTS

6.1 Data Storage & Sharing

- Shared information shall be held for a maximum of one year but not less than 6 months after the issuance of a licence/BOPA
- The owner of the information at this stage is the Child Entertainment & Employment officer
- As per information shared for a particular licence or BOPA request, the share of information shall be a one off exercise unless where variations are requested by the licence/BOPA applicant

6.2 Data security arrangements:

- Information will be stored electronically within the local authority's secure servers
- Where hard documents are required, they are stored away in locked facilities within the office premises of the local authority
- Documents pertaining to shared information shall not be taken home by employees
- Any identified data breaches shall be reported to any cosignatories to this agreement. Each organisation undertakes to carry out under its own policies an incident management investigation, and report on

findings relevant to the sharing of personal data taken in view of this ISA.

6.3. Data Transfer:

- Information transfers shall be done in encrypted messages
- Where required, information will be sent by recorded post

6.4 Data Access & Review:

- This ISA will be reviewed annually.
- If any significant change takes place making the agreement unreliable, then the agreement will be updated as required and a new version issued.

Please Add Sections 7 and 8 Where You are or are Likely to Process Personal Data. These fields provide for a fuller explanation and guide to this data sharing agreement.

7. DATA PROTECTION LEGISLATION AND GUIDANCE

The DPA governs the protection and use of personal information identifying living individuals. The DPA gives individuals rights in relation to the handling of their personal data by organisations. Organisations must handle this information in accordance with standards in the DPA known as the Data Protection Principles. These are outlined in Appendix B

This Agreement does not seek to supersede the principles and regulatory framework that is the DPA, any subordinate or related legislation, orders or judgements. In the event of conflict between any part of this Agreement and any legislative or policy requirement in place, the latter will take precedence and that part of the Agreement deemed to be in conflict will be considered suspended until the Agreement is reviewed and, if necessary, revised.

8. GENERAL DATA PROTECTION PRINCIPLES

8.1 Lawfulness of processing of data

Participating organisations/departments should ensure that the sharing of personal data under this protocol is lawful and does not contravene any lawful power to which they may be subject. Where the organisation's functions are determined by statute (eg. local authorities or other statutory bodies) then it must be ensured that they are not acting *ultra vires* in participating in this data sharing arrangement. In addition, participating organisations/departments must ensure that the sharing of data meets at least one of the conditions of processing in Schedule 2 of the DPA (see Appendix C for list).

8.2 Notification under the Data Protection Act 1998

It is the responsibility of each participating organisation to ensure that the handling of personal data under this protocol is included in their Notification to the Office of the Information Commissioner as required under the DPA.

8.3 Informing data subjects/seeking consent

Individuals **must** be made aware that their information will be shared for the purpose of this Agreement. It is a requirement of Principle 1 of the DPA that where an organisation obtains personal data, they must ensure that the individual is aware not only of the **reason** for which such information is being collected but also aware of with **whom** it may be shared. This need only be done once; it is neither practicable nor necessary to seek an individual's specific consent each time that information is passed on for a particular purpose that has been defined in this protocol. Each signatory to this Agreement will need to demonstrate that this requirement has been fulfilled.

In some cases, where **sensitive personal data** is to be shared, **participating organisations/departments will need to obtain explicit consent f**or the sharing unless they can satisfy another condition under Schedule 3 of the DPA (see Appendix D).

In either case where consent has been sought, it is important to note that individuals are entitled to withdraw their consent at any time. Where an individual contacts the participating organisation/department to withdraw their consent - subject to any exemptions that may apply - the participating organisation/department **must** advise all other parties to this Agreement and the individual's data must not be handled for the purpose(s) of this data sharing arrangement.

8.4 Secondary purposes

Principle 2 of the DPA states that "personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or these purposes".

The purpose for sharing data under this protocol should be compatible with the purpose for which the personal data was originally obtained by the participating organisation/department. Where the data is being shared for a non-compatible purpose, each owner of the data must seek the permission from the data subject for the secondary use of their personal data. This should be done prior to any sharing for secondary use, or as reasonably practicable.

8.5 Minimal identifiable information

In line with Principle 3 of the DPA "personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed." It is essential that the data collected by the organisation/department and that which is shared with other parties is the minimum identifiable information necessary for the purpose of this data sharing arrangement.

8.6 Accuracy of the data

It is the responsibility of each participating organisation/department to ensure and maintain the accuracy of personal information they share with other organisations under this Agreement. Where an organisation/department becomes aware that information they have provided may be inaccurate, they **must** take steps to inform all participating organisations/departments of the updated data.

8.7 Disclosure

Personal information should only be disclosed for the purpose identified in section 4 (Purpose for which information is to be shared) and in accordance with what the individual has been told. There are exceptions if the information is required for the following purposes:

- the disclosure is necessary for the prevention of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or of any imposition of a similar nature (s.29)
- the disclosure consists of information which is required by law to be made publicly available (s.34)
- the disclosure is required by law or by order of the court (s.35(1))
- the disclosure is made in connection with legal proceedings (s.35(2))

Outside of section 35(1) none of the above caveats are mandatory, which means that disclosures will have to be considered on a case-by-case basis. Generally, disclosure should be proportional and must consider the Rights of third parties whose personal data may also be present. Each signatory should ensure that they consult with their Data Protection officers, as well as document and inform other signatories of the disclosure. Where the information has been provided by a medical practitioner, the owner of the data will be responsible for ensuring that their consent has been obtained to the disclosure.

8.8 Security issues

Each participating organisation/department must take all reasonable care and employ appropriate physical, technical and organisational safeguards to the personal data under this data sharing arrangement. Participating organisations/departments must agree on the standards required for protecting the data, for example, the storage safeguards for information in hardcopy and electronic format, security of data in transmission, security standards for access to the data. Higher safeguards will be required where the personal data is of a sensitive nature.

Staff should only have access to personal data in order to perform their duties in connection with one or more of the purposes defined in section 3 (Purpose for which information is to be shared). Technical and physical safeguards should be in place to restrict access to the information only to authorised staff for example, password control. These should be in line with agreed policies and procedures

8.9 Data Protection Right of Subject Access

Under the DPA, individuals have rights to have access to personal information about them held by any organisation. Subject access requests must be fulfilled within 40 calendar days. Each participating organisation/department has responsibility for ensuring that individuals are provided with access to personal information held about them in accordance with the requirements of the Act. If this agreement relates to Triborough Shared Services please refer to the Triborough Information Management Portal for more advice.

8.10 Retention of personal data and non-personal data

Unless a statutory period applies, data which is kept for the purpose of this data sharing arrangement should only be kept for as long as necessary in line with agreed policies. Participating organisations/departments should agree and document a standard period for which the information will be retained, a procedure for how the data will be reviewed and agree on secure disposal methods.

8.11 Other Related Legislation

The Common Law Duty of Confidentiality

The Common law duty of confidentiality may apply to a large amount of information obtained by an organisation. As a general principle the duty arises where a person receives information in situations where it is known or can be taken to be known that the information is to be treated as confidential.

Whenever information is obtained in circumstances where a duty of confidence is to be inferred, there is a legal duty to respect the confidentiality of information provided and not to disclose it to third parties without consent, unless an overriding public interest requires it. Under common law there is a duty to act reasonably and in a manner that is proportionate to the aim. Information obtained in confidence should not be disclosed to a greater extent than is necessary in the interests of the individual.

Generally, it will be possible to satisfy legal obligations under the common law duty of confidentiality if the personal information is handled in a manner that complies with the obligations as set out in the Data Protection Act.

The Human Rights Act 1998

The Human Rights Act prohibits interference by a public authority with the private and family life of individuals, their homes and correspondence, save where that interference is lawful and necessary in a democratic society, public safety, the protection of rights and freedoms of others, the prevention of disorder or crime and the protection of health and morals.

Interference with an individual's privacy must not be disproportionate even where it is in pursuit of such aims as allowed by the Human Rights Act. In addition, the handling of an individual's personal information should only be limited to pursue the objectives for which the information was collected.

Freedom of Information Act 2000

The Freedom of Information Act provides for a general right of access to official information held by public authorities (subject to the exemptions contained in the Act), and as each of the partners is a public authority there is a statutory duty to handle requests for information in accordance with the framework of the Act. Where the data sharing agreement involves another public authority(s), it will be the duty of the recipient public authority to handle the request in accordance with the legislation. Each signatory who is subject to the Act should make proper arrangements to enable information to be shared and disclosed in relation to non-personal data.

9. ACCOUNTABILITY UNDER THIS PROTOCOL

9.1 Authorised officer

This Agreement must be signed by an authorised officer for each participating organisation/department (see Appendix A).

9.2 Designated senior officer

Each authorised officer should nominate at least one senior officer within each participating organisation/department responsible for agreeing amendments to the Agreement, monitoring and reviewing its operation and ensuring compliance. Designated seniors officers and contact details are listed at Appendix E.

9.3 Staff obligations

It is the responsibility of each participating organisation/department to ensure that staff with authorised access to the data covered by this Agreement are aware of their obligations under the DPA to safeguard that information. Staff should be aware that breach of this protocols contained within this Agreement could be a matter for disciplinary action and may provide grounds for a complaint under the DPA against them which may result in criminal or civil action against them.

9.4 Review of the protocol

All elements of this protocol will be reviewed every 12 months.

9.5 Withdrawal from the Agreement

If any party wishes to withdraw from this Agreement, they must give six weeks written notice of this intent. Letters will be addressed to the signatories of the protocol at the addresses shown on the Agreement (Appendix E). Individuals whose data has been hitherto shared must be informed where a participating organisation/department has withdrawn from the data sharing arrangement.

Any party who withdraws **must** ensure that all data is reviewed and deleted.

10. ADDITIONAL CLAUSES

[Clauses can be added as required]

Appendix A: The Agreement

Protocol for sharing personal information between ACE Westminster City Council and Hertfordshire Music Service

Agreement

We the undersigned do hereby agree to implement the full range of measures outlined in this protocol.

For and on behalf of ACE, Westminster City Council

Signature: 

Name: RICHIE ADEYEYE

Position: LEAD ADVISER

Address: 2nd Floor, Kensington Town Hall

Hornton Street

London W8 7NX

Date:

* For and on behalf of

Signature: _____

Name: _____

Position: _____

Address: _____

_____

_____

Date: _____

(* duplicate as necessary for each participating organisation)

APPENDIX B: THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix C: Conditions Relevant for Purposes of the First Principle: Processing of any Personal Data

1. The data subject has given his consent to the processing.

2. The processing is necessary-
    a. for the performance of a contract to which the data subject is a party, or
    b. for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary-
    a. for the administration of justice,
    b. for the exercise of any functions conferred on any person by or under any enactment,
    c. for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
    d. for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

    (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Appendix D: Conditions Relevant For Purposes of the First Principle: Processing of Sensitive Personal Data

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary-

(a) in order to protect the vital interests of the data subject or another person, in a case where-

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing-

(a) is carried out in the course of its legitimate activities by any body or association which-

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing-

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary-

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by-

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing-

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Appendix E: Designated Officers

PARTICIPATING ORGANISATION/DEPARTMENT	NAME OF DESIGNATED OFFICER	POSITION AND RESPONSIBILITY	CONTACT DETAILS