

## **Hackney Play Association Confidentiality Policy**

This policy on confidentiality has been developed to ensure that Hackney Play Association protects all information provided by service users and staff in accordance with the legal principles and good practice of confidentiality, data protection and information sharing. Hackney Play Association recognises the importance of maintaining a confidential service given the personal and sensitive nature of information provided by parents regarding children and young people; by the children and young people themselves. The aim of the policy will be to ensure that the principles of confidentiality are maintained in all aspects of processing, storage and sharing of information.

### **1. General principles**

- 1.1. Hackney Play Association (HPA) recognises that staff (including employees, volunteers, trustees, and students) can gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and staff may have to exercise common sense and discretion in identifying whether information is expected to be confidential. This policy aims to give guidance but if in doubt, seek advice from your line manager.
- 1.2. Staff are able to share information with their line manager in order to discuss issues and seek advice.
- 1.3. Staff will avoid exchanging personal information or comments about individuals with whom they have a professional relationship.
- 1.4. Staff will avoid talking about organisations or individuals in social settings.
- 1.5. Staff will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.
- 1.6. There may be circumstances where staff would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem. The organisation's consent must be sought before discussing the situation, unless the colleague is convinced beyond doubt that the organisation would not object to this. Alternatively, a discussion may take place with names or identifying information remaining confidential.

- 1.7. Where there is a legal duty on HPA to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made.

## **2. Why information is held**

- 2.1. Most information held by HPA relates to children and their families, staff, other individuals, voluntary and community organisations, self-help groups, volunteers, students, employees, trustees or services which support or fund them.
- 2.2. Information is kept to enable HPA to understand the history and activities of individuals or organisations in order to deliver the most appropriate services and to operate effectively.
- 2.3. HPA has a role in putting people in touch with voluntary and community organisations and keeps contact details which are passed on to any enquirer, except where the group or organisation expressly requests that the details remain confidential.
- 2.4. Information about participants on training courses may be given to their employer, training organisation and college, but to no one else.
- 2.5. Information about ethnicity and disability of users is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

## **3. Access to information**

- 3.1. Information is confidential to HPA as an organisation and may be passed to colleagues, line managers or trustees to ensure the best quality service for users.
- 3.2. Where information is sensitive, i.e. it involves disputes or legal issues, it will be confidential to the employee dealing with the case and their line manager. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled to access the information and the name of the individual or group who may request access to the information.
- 3.3. Staff will not withhold information from their line manager unless it is purely personal.
- 3.4. Children and parents/carers may have sight of HPA records held in their name.
- 3.5. Employees may have sight of their personnel records by giving 14 days' notice in writing to the Director.
- 3.6. When photocopying or working on confidential documents, colleagues must ensure people passing do not see them. This also applies to information on computer screens.

#### 4. Storing information

- 4.1. General non-confidential information about organisations is kept in unlocked filing cabinets and in computer files with open access to all HPA staff.
- 4.2. Personnel information on employees, volunteers, students and other individuals working within HPA will be kept in lockable filing cabinets or on password protected computers by line managers and will be accessible to the Director and Chair of HPA Trustees.
- 4.3. In an emergency situation, the Director or HPA Chair may authorise access to files by other people.

#### 5. Duty to disclose information

- 5.1. There is a legal duty to disclose some information including:
  - 5.1.1. Child abuse and safeguarding concerns which must be dealt with as outlined in the HPA Safeguarding Policy
  - 5.1.2. HPA uses the guidance set out in *Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers*, published by the Government in 2015 that information sharing must be: necessary and proportionate, relevant, adequate, accurate, timely, secure and recorded.
  - 5.1.3. Drug trafficking, money laundering or acts of terrorism will be disclosed to the police.
- 5.2. In addition staff believing an illegal act has taken place or that a user is at risk of harming themselves or others, must report this to their line manager or the Director who will decide the next steps to take.

#### 6. Disclosures

- 6.1 HPA complies fully with the DBS Code of practice regarding the correct handling, use, storage, retention and disposal of Disclosure information.
- 6.2 Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a **criminal offence** to pass this information to anyone who is not entitled to receive it.
- 6.3 Documents will be kept for six months and then destroyed by secure means. Photocopies will not be kept. However, HPA may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

## **7. Data Protection Act**

7.1. Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principles. These are that personal data must be:

- Obtained and processed fairly and lawfully.
- Held only for specified purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept longer than necessary.
- Processed in accordance with the Act.
- Kept secure and protected.
- Not transferred out of Europe.

7.2 Children and Young People have the right to know what information is held about them

## **8. Breach of confidentiality**

8.1. Employees who are dissatisfied with the conduct or actions of other colleagues or HPA should raise this with their line manager and not discuss their dissatisfaction outside of HPA.

8.2. Staff accessing unauthorised files or breaching confidentially may face disciplinary action.

## **9. Whistle blowing**

9.1. Where the Finance Worker has concerns about the use of HPA funds, he or she may refer directly to the Chair or Treasurer outside the usual grievance procedure.

9.2. All staff hold the right to inform either his or her manager or one of the trustees if they believe that HPA is being brought into disrepute by the actions of another colleague or trustee. Further information is available in HPA's whistleblowing policy.

Further information and advice about Data Protection can be sought from the Information Commissioners Office at <http://ico.org.uk/>

See also: *Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers*, published by the Government in 2015.

## **Appendix 1:**

### ***Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers, HM Government, 2015***

#### **The seven golden rules to sharing information**

1. Remember that the Data Protection Act 1998 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.
5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

#### **The principles**

The principles set out below are intended to help practitioners working with children, young people, parents and carers share information between organisations.

Practitioners should use their judgement when making decisions on what information to share and when and should follow organisation procedures or consult with their manager if in doubt.

**The most important consideration is whether sharing information is likely to safeguard and protect a child.**

## **Necessary and proportionate**

When taking decisions about what information to share, you should consider how much information you need to release. The Data Protection Act 1998 requires you to consider the impact of disclosing information on the information subject and any third parties. Any information shared must be proportionate to the need and level of risk.

## **Relevant Only**

Information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make sound decisions.

## **Adequate**

Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

## **Accurate**

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

## **Timely**

Information should be shared in a timely fashion to reduce the risk of harm. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore harm to a child. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

## **Secure**

Wherever possible, information should be shared in an appropriate, secure way. Practitioners must always follow their organisation's policy on security for handling personal information.

## **Record**

Information sharing decisions should be recorded whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary. In some circumstances this may be indefinitely, but if this is the case there should be a review process.