



**ELHAP – A SPECIAL NEEDS ADVENTURE PLAYGROUND**  
119, Roding Lane North  
Woodford Bridge  
Essex  
IG8 8NA

Telephone: 020 8550 2636  
Fax: 020 8550 2683  
Email: [info@elhap.org.uk](mailto:info@elhap.org.uk)  
Website: [www.elhap.co.uk](http://www.elhap.co.uk)

---

## **Data Protection Policy**

---

### **Contents**

1. General Statement
2. Enquiries
3. Fair Obtaining and Processing
4. Registered Purposes
5. Data Integrity
6. Subject Access
7. Processing Subject Access Requests
8. Authorised Disclosures
9. Data and Computer Security
10. Further Information

---

### **1. General Statement**

The ELHAP – A Special Needs Adventure Playground (henceforth referred to as 'ELHAP') Board of Trustees has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with the Data Protection Act (1998) and all other statutory provisions.

The ELHAP Board of Trustees intend to comply fully with the requirements and principles of the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

### **2. Enquiries**

Information about the ELHAP Data Protection Policy is available from the Centre Manager. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)).

### **3. Fair Obtaining and Processing**

ELHAP undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held,

the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

**“processing”** means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

**“data subject”** means an individual who is the subject of personal data or the person to whom the information relates.

**“personal data”** means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

**“parent”** has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a service user.

#### **4. Registered Purposes**

The Data Protection Registration entries for ELHAP are available for inspection, by appointment, at the ELHAP general office. Explanation of any codes and categories entered is available from the Centre Manager, who is the person nominated to deal with Data protection issues at ELHAP. Registered purposes covering the data held at ELHAP are listed on the ELHAP registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

#### **5. Data Integrity**

ELHAP undertakes to ensure data integrity by the following methods:

##### **a) Data Accuracy**

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs ELHAP of a change of circumstances their computer record will be updated as soon as is practicable. On occasion, a printout of their data record will be provided to data subjects so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, ELHAP will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the ELHAP Board of Trustees for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

##### **b) Data Adequacy and Relevance**

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, ELHAP will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

### **c) Length of Time**

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Centre Manager to ensure that obsolete data are properly erased.

## **6. Subject Access**

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a “data subject”, ELHAP’s policy is that:

- Requests from a “data subject” will be processed as any subject access request as outlined below and the copy will be shown to the “data subject” at a pre-arranged appointment, unless it is clear that the “data subject” does not understand the nature of the request.
- Requests from “data subjects” who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child/young person/adult will be processed as requests made on behalf of the “data subject” (the service user) and the data will be shown to the requesting parent at a pre-arranged appointment.
- Requests for copies of personal data will normally be considered after access has been completed via a pre-arranged appointment (as detailed above). Copies will be sent by registered post in a sealed envelope.

## **7. Processing Subject Access Requests**

Requests for access must be made in writing to the ELHAP Centre Manager at the above address.

Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject’s name, the name and address of requester (if different), the type of data required (eg Service Users Records, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

## 8. Authorised Disclosures

ELHAP will, in general, only disclose data about individuals with their consent. However there are circumstances under which ELHAP's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Service User data disclosed to authorised recipients related to education, health, social services and administration necessary for ELHAP to perform its statutory duties and obligations.
- Service User data disclosed to authorised recipients in respect of their health, safety and welfare.
- Service User data disclosed to parents/carers in respect of their child's/young people's/adult's progress, achievements, attendance, attitude or general demeanour within ELHAP.
- Staff data disclosed to relevant authorities eg in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside of ELHAP.
- Only authorised staff are allowed to make external disclosures of personal data. Data used within ELHAP by staff will only be made available where the person requesting the information is a professional legitimately working with ELHAP who **need to know** the information in order to do their work. ELHAP will not disclose anything on Service Users' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child/adult abuse.

A “**legal disclosure**” is the release of personal information from the computer to someone who requires the information to do his or her job within or for the ELHAP, provided that the purpose of that information has been registered.

An “**illegal disclosure**” is the release of information to someone who does not need it, or has no right to it, or one which falls outside ELHAP's registered purposes.

## 9. Data and Computer Security

ELHAP undertakes to ensure security of personal data by the following general methods:

### a) Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks etc. Only authorised persons are allowed in the General Office. Disks, tapes and printouts are locked away securely when not in use.

Visitors to ELHAP are required to sign in and out, and are, where appropriate, accompanied.

### **b) Logical Security**

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (ie security copies are taken) regularly.

### **c) Procedural Security**

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are aware in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the ELHAP Board of Trustees and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in ELHAP should in the first instance be referred to ELHAP Centre Manager.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

## **10. Further Information**

Further details on any aspect of this policy and its implementation can be obtained from the ELHAP Centre Manager

**Implemented by the ELHAP Board of Trustees  
3<sup>rd</sup> October 2005**