

**Mobile Education Partnerships**

**GDPR COMPLIANCE and DATA PROTECTION POLICY**

**Originated: July 2017**

**Adopted: July 2017**

**Next Revision: April 2020**

**Next Revision: April 2022**

**Approved by: Board of Directors**

**Document Status: Charity Policy**

**Registered Charity No: 1115837**

**Registered Company No: 5664251**

**Registered Office: 16, The Green, Hett, Durham DH6 5LX**

**Contents**

1. **Introduction**
2. **Data protection officer**
3. **Data protection principles**
4. **Data subject access requests**
5. **Individual’s obligations regarding personal information**
6. **Consequences of non-compliance**
7. **Review of procedures**
8. **Data Protection Act 1998**
9. **Data Breaches**

**1.0 INTRODUCTION**

Mobile Education Partnership is committed to all aspects of data protection and takes seriously its duties, and the duties of its individuals, under the Data Protection Act 1998. This policy sets out how MEP deals with personal data, including personnel files and data subject access requests, and individuals' obligations in relation to personal data.

**2.0 Data Protection Officer**

The Company Secretary is MEP's data protection officer and is responsible for the implementation of this policy. If individuals have any questions about data protection in general, this policy or their obligations under it, they should direct them to the Company Secretary, contactable at admin@mobileeducationpartnerships.org

**3.0 Data Protection Principles**

The Data Protection Act 1998 requires that eight data protection principles be followed in the handling of personal data. These principles require that personal data must:

* be fairly and lawfully processed
* be processed for limited purposes and not in any manner incompatible with those purposes
* be adequate, relevant and not excessive
* be accurate
* not be kept longer than is necessary
* be processed in accordance with individuals' rights
* be secure
* not transfer between countries without adequate protection

**3.1 Personal data and Email addresses**

The Data Protection Act 1998 applies only to information that constitutes "personal data". Information is "personal data" if it:

identifies a person, whether by itself, or together with other information in MEP's possession, or is likely to come into its possession; and

is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

Consequently, automated and computerised personal information about individuals held by employers is covered by the Act. Personal information stored physically (for example, on paper) and held in any "relevant filing system" is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.

Supporters and others whose email addresses we use are asked if they wish us to continue contacting them.

**3.2 The use of personal information**

The Data Protection Act 1998 applies to personal information that is "processed". This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it.

**3.3 Sensitive personal data**

"Sensitive personal data" is information about an individual; everyone has the right to enquire what information is being held concerning their own records

* racial or ethnic origin;
* political opinions;
* religious beliefs or other beliefs of a similar nature;
* physical or mental health or condition;
* sex life;
* commission or alleged commission of any criminal offence; and
* proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

MEP will not retain sensitive personal data without the express consent of the individual in question.

MEP will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles. MEP enters into discussions about a merger or acquisition with a third party, MEP will seek to protect individuals' data in accordance with the data protection principles.

1. **Computer Use**
2. There is no network set-up either between directors or in any of the offices abroad
3. There are 3 levels of access to Google Drive:
	1. Directors
	2. Manager
	3. Trainers

Passwords will be changed at regular intervals especially when a director or manager no longer works with MEP At the time of this revision, discussion is underway, to revise how we might share information whether by Google Drive or by some other method. This policy will be updated as and when this is applicable.

Directors have access to all 3 levels. No personal information eg identity documents, CVs or references, should be posted on any of these drives. Any information necessary for interviews should be shared directly between directors, then deleted after the interviews for unsuccessful candidates; information on successful candidates to be kept by Company Secretary until such time that the interviewee no longer works with MEP. Any other confidential information including agreements, to be kept solely by Company Secretary

**3.4 Personnel files**

An individual's personnel file is likely to contain information about his/her work history with MEP and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the individual including address details and national insurance number.

There may also be other information about the individual located within MEP, for example in his/her line manager's inbox or desktop, or within documents stored in a relevant filing system.

 MEP will ensure that personal information about an individual, including information in personnel files, is securely retained. MEP will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords.

Where laptops are taken off site, individuals must follow MEP's relevant policies relating to the security of information and the use of computers for working at home/bringing your own device to work.

**4.0** **Data subject access requests**

When an individual starts working with MEP they will be given access to the Trainers’ Drive Please see 3.3.a above for possible changes

MEP will inform each individual of:

* the types of information that it keeps about him/her;
* the purpose for which it is used; and
* the types of organisation that it may be passed to

An individual has the right to access information kept about him/her by MEP, including personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the individual is the focus of the email and documents that are about the individual.

The Company Secretary is responsible for dealing with data subject access requests.

MEP will allow the individual access to any personal information.

**5.0 Individual’s obligations regarding personal information**

If an individual acquires any personal information in the course of his/her duties, he/she must ensure that:

* the information is accurate and up to date, insofar as it is practicable to do so;
* the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
* the information is secure.
* In particular, an individual should ensure that he/she:
* uses password-protected and encrypted software for the transmission and receipt of emails;
* locks files in a secure cabinet.

Where information is disposed of, individuals should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an individual's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Individuals should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an individual acquires any personal information in error by whatever means, he/she shall inform the Company secretary immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within MEP.

Where an individual is required to disclose personal data to any other country, he/she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact the Company Secretary.

An individual must not take any personal information away from MEP's premises save in circumstances where he/she has obtained the prior consent of the company Secretary

If an individual is in any doubt about what he/she may or may not do with personal information, he/she should seek advice from the company Secretary. If he/she cannot get in touch with the Company Secretary, he/she should not disclose the information concerned.

**6.0 Consequences of non-compliance**

All individuals are under an obligation to ensure that they have regard to the eight data protection principles (see [above](http://www.xperthr.co.uk/policies-and-documents/data-protection-policy/19379/?c=2513#principles)) when accessing, using or disposing of personal information. It may also result in disciplinary action up to and including dismissal. For example, if an individual accesses another individual's employment records without the requisite authority, MEP will treat this as gross misconduct and instigate its disciplinary procedures.

**6.1 Taking employment records off site**

An individual must not take employment records off site (whether in electronic or paper format) without prior authorisation from the Company Secretary.

Any individual taking records off site must ensure that he/she does not leave his/her laptop, other device or any hard copies of employment records on the train, in the car or any other public place. He/she must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

**7.0 Review of procedures**

MEP will review and ensure compliance with this policy at regular intervals.

**8.0** **Data Protection Act 1998**

The Data Protection Act 1998 lists eight data protection principles which state that organisations must:

* process personal data fairly and lawfully (ie personal information must not be obtained or used unless either the individual has consented or one of a limited range of conditions is met);
* obtain and process data only for one or more specified and lawful purposes (ie use personal information only for specified agreed purposes);
* ensure that data is adequate, relevant and not excessive (ie not store more information than is necessary about a person);
* ensure that data is accurate and, where necessary, kept up to date;
* not keep data for longer than is necessary;
* process data in accordance with the rights of individuals;

keep data secure

* not transfer between countries without adequate protection
1. **Data Breaches**

The amount of data that MEP holds on anyone is minimal and doesn’t extend beyond personal information given at interview. No social media data is collated and email addresses are only kept and used for internal purposes. Any ‘data breach’ would only be as part of a larger breach and would be investigated as part of a wider ranging investigation.

MEP has provided this data protection policy to encourage a "data protection culture" among staff for the safeguarding and for the management of information.

*\*This document to be read in conjunction with the* **Consent to the Use of Personal Data**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Personnel | Position | References(oral/written)Yes/No | DBS checked(non-UK where and if appropriate) | Placement(eg Mae Sot, Mawlamyine) | From(date) | To(date) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Copy of updated table (above) to be kept in Directors’ area of Google Drive