DATA PROTECTION POLICY

Policy Title	Data Protection Policy
Issue Date	April 2024
Author	Helen Knight
Review Date	April 2025

The UMBRELLA HUB

THE UMBRELLA HUB COMMUNITY CIC

DATA PROTECTION POLICY

CONTENTS

THE UMBRELLA HUB COMMUNITY CIC

DATA PROTECTION POLICY

1.	**INTRODUCTION**
	The Umbrella Hub Community CIC needs to keep certain information about staff, clients and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, legal obligations to the government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Organisation must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall: • Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met. • Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose. • Be adequate, relevant and not excessive for those purposes. • Be accurate and kept up to date. • Not be kept for longer than is necessary for that purpose. • Be processed in accordance with the data subject's rights. • Be kept safe from unauthorised access, accidental loss or destruction. • Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

	The Organisation and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Organisation has developed this Data Protection Policy.
2.	**TERMINOLOGY**
	Data – information which is: • being processed by means of equipment operating automatically in response to instructions given for that purpose; • recorded with the intention that it should be processed by means of such equipment; • recorded as part of a relevant filing system (a structured system); or • forms part of an accessible record. This includes such things as manual index card files, microfiche, etc. **The Data Controller –** The Organisation as a Body is the Data Controller under the Act, and the CO Directors are therefore ultimately responsible for implementation. **Personal Data -** data which relates to a living individual who can be identified. **The data subject -** The person identified, or who can be identified from the personal data or when used in conjunction with other data held by the data controller, or is likely to come into their possession. **Processing** - means obtaining, recording or holding the information or carrying out an operation on the information.

	Recipient - any person to whom the data is disclosed, including another staff member of the data controller. **Source** - a recognised and lawful source of personal data collection. **Disclosure** - a recognised and lawful recipient of personal data (in compliance with the purpose of processing).
3.	**STATUS OF THE POLICY**
	It is a condition of employment that staff will abide by the rules and policies made by the Organisation from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings. **Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the HR Manager. If the matter is not resolved it should be raised as a formal grievance.**
4.	**NOTIFICATION OF DATA HELD AND PROCESSED**
	All staff and clients and other Organisation users are entitled to know • what information the Organisation holds and processes about them and why. • how to gain access to it. • how to keep it up to date. • what the Organisation is doing to comply with its obligations under the 1998 Act. The Organisation will therefore provide all persons covered by this policy with relevant personal information from time to time for checking, particularly in the

	case of staff information which may change over time e.g. residential address, qualifications etc.
5.	**RESPONSIBILITIES OF STAFF**
	• Checking that any information that they provide to the Organisation in connection with their employment is accurate and up to date. • Informing the Organisation of any changes to information, which they have provided, i.e. changes of address • Checking the information that the Organisation will send out from time to time, giving details of some information kept and processed about staff • Informing the Organisation of any errors or changes. The Organisation cannot be held responsible for any errors/changes unless the staff member has informed the Organisation of them. If and when, as part of their responsibilities, staff collect information about other people, they must comply with the guidelines for staff. See Appendix C
6.	**DATA SECURITY**
	All staff are responsible for ensuring that: • Any personal data which they hold is kept securely. • Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

	Personal information should be: • kept in a locked filing cabinet; or • in a locked drawer; or • if it is computerised, be password protected; or • encrypted.
7.	**CLIENT OBLIGATIONS**
	Clients must ensure that all personal data provided to the Organisation is accurate and up to date. They must ensure that change of address etc. is notified to the Organisation as appropriate.
8.	**RIGHTS TO ACCESS INFORMATION**
	Staff and clients and other users of the Organisation have the right to access any personal data which are being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the Organisation 'Access to Data Request' form, Appendix D (staff) and Appendix E (clients) and hand it to the HR Manager. The Organisation aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.
9.	**PUBLICATION OF ORGANISATION INFORMATION**
	Information which is already in the public domain is exempt from the 1998 Act. It is the Organisation policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

	• List of staff • Photographs of Senior Postholders The Organisation's internal phone list will not be a public domain. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the HR Manager.
10.	**SUBJECT CONSENT**
	In many cases, the Organisation can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to the Organisation processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974. Some jobs or courses will bring applicants into contact with children, including young people (children) between the ages of 13 and 18. The Organisation has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The Organisation also has a duty of care to all staff and clients and must therefore make sure that staff and those who use the Organisation facilities do not pose a threat or danger to other users. The Organisation will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The Organisation will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

	Therefore, all prospective staff and clients will be asked to sign a Consent to Process statement, regarding particular types of information when an offer of employment or support respectively is made. A refusal to sign can result in the offer being withdrawn.
11.	**PROCESSING SENSITIVE INFORMATION**
	Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the Organisation is a safe place for everyone, or to operate other Organisation policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students are asked to give express consent for the Organisation to do this. Offers of employment or support may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Directors.
12.	**RETENTION OF DATA**
	The Organisation keeps some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so.
13.	**CONCLUSION**
	Compliance with the 1998 Act is the responsibility of all members of the Organisation. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Organisational facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the CEO.

Approved by	
Please Print	
Position	
Date	