DATA PROTECTION POLICY AND PROCEDURE

This policy is divided into two parts: Part One relates to the organisation's 'internal' data protection (e.g. Data concerning employees, governors and volunteers/members); Part Two relates to the data concerning service users and members of the public.

PART ONE: ORGANISATION 'INTERNAL' DATA

1.0 **Purpose**

1.1 In the course of HWD CIC work, directors, members of staff and volunteers (hereinafter called representatives) may come into contact with or use confidential information about employees, clients, customers and suppliers, for example their names and home addresses. The Data Protection Act 1998 contains principles affecting employees' and client's personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel or service user 's files that form part of a structured filing system.

1.2 The purpose of these rules is to ensure that representatives do not breach the Act. If anyone is in any doubt about what can or cannot be disclosed and to whom, they should not disclose the personal information until they have sought further advice from HWD CIC's Data Protection Officer. Representatives should be aware that they may be criminally liable, through the powers granted to the Information Commissioner's Office, if they knowingly or recklessly disclose personal data in breach of the Act.

1.3 A serious breach of data protection is also a disciplinary offence and will be dealt with under HWD CIC's disciplinary procedure, for example, if another employee's personnel records is accessed without authority or if a service user's confidentiality is breached, this constitutes a gross misconduct offence and could lead to summary dismissal.

The Data Protection Act 1998 and the Data Protection (Amendment) Act 2003 cover both:

- Information HWD CIC stores and processes on its governors, employees and volunteers/members; and
- Information HWD CIC stores and processes on its service users or members of the public

2.0 **Data protection and HWD CIC representative information**

2.1 The Eight Data Protection Principles

There are eight data protection principles that are central to the Act. HWD CIC and all its representatives must comply with these principles at all times in their information-handling practices. In brief, the principles say that personal data must be:

2.1.1 Processed fairly and lawfully and must not be processed unless certain criteria are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the representatives or service user and consists of information relating to:

i. Race or ethnic origin.
ii. Political opinions and trade union membership.
iii. Religious or other beliefs.
iv. Physical or mental health condition.
v. Sexuality

vi. Criminal offences, both committed and alleged.

2.1.2 Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.

2.1.3 Adequate, relevant and not excessive. HWD CIC will review personnel files on a regular basis to ensure they do not contain a backlog of out-of-date information and to check there is a sound business reason requiring information to continue to be held.

2.1.4 Accurate and kept up-to-date. If personal information changes, for example a representative changes address or gets married and changes their surname, they must inform their line manager as soon as practicable so that HWD CIC's records can be updated. HWD CIC cannot be held responsible for any errors unless the representative has notified HWD CIC of the relevant change.

2.1.5 Not kept for longer than is necessary. HWD CIC will keep personnel files for no longer than six years after termination of employment, or ten years if the employee worked with children and young people. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data that HWD CIC decides it does not need to hold for a period of time will be destroyed after approximately one year. Data relating to unsuccessful job applicants will only be retained for a period of six months.

2.1.6 Processed in accordance with the rights of employees under the Act.

2.1.7 Secure. Technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Personnel files are confidential and are stored in locked filing cabinets. Only authorised employees are permitted to have access to these files. Files must not be removed from their normal place of storage without good reason. Personal data stored on removable storage media must be kept in locked filing cabinets. Personal data held on computer must be stored confidentially by means of password protection, encryption or coding and again only authorised employees are permitted to have access to that data. HWD CIC has network back-up procedures to ensure that data on computer cannot be accidentally lost or destroyed.

2.1.8 Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.

3.0 Your consent to personal information being held

HWD CIC holds personal data about representatives and their consent to HWD CIC processing their personal data is a condition of their employment or voluntary role. Therefore, by agreeing to a contract of employment, or signing a Volunteer Agreement, a representative also agrees to their personal data being held and processed. HWD CIC holds limited sensitive personal data about its employees and, by signing a contract of employment, they give their explicit consent to HWD CIC's holding and processing of that data, for example sickness absence records, health needs and equal opportunities monitoring data.

4.0 Representatives' right to access personal information

4.1 Under the provisions of the Act, representatives have the right, on request, to receive a copy of the personal data that HWD CIC holds about them, including their personnel file to the extent that it forms part of a relevant filing system, and to demand that any inaccurate data be corrected or removed. A representative has the right on request:

a. To be told by HWD CIC whether and for what purpose personal data about them is being processed.
b. To be given a description of the personal data and the recipients to whom it may be disclosed.
c. To have communicated in an intelligible form the personal data concerned, and any information available as to the source of the personal data.
d. To be informed of the logic involved in computerised decision-making.

4.2 The sharing of personal data such as home address, personal contact details may be necessary where deemed proportionate and for the purpose of pursuing business reasons in relation to HWD CIC policies and procedures which govern the conduct, pay and benefits of employees in the workplace.

4.3 Upon request, HWD CIC will provide a representative with a written statement regarding the personal data held about them. This will state all the types of personal data HWD CIC holds and processes about them and the reasons for which the data is processed. If the representative wishes to access a copy of any personal data being held about them, they must make a written request for this and HWD CIC reserves the right to charge a fee of up to £10 per request. To make a request, please apply to HWD CIC's Data Protection Officer.

4.4 If a representative wish to make a complaint that these rules are not being followed in respect of personal data HWD CIC holds about them, they should raise the matter with HWD CIC's Data Protection Officer. If the matter is not resolved to their satisfaction, it may then be raised as a formal grievance under HWD CIC's grievance procedure.

5.0 Data Protection and Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE)

5.1 HWD CIC has a legislative duty to provide personal and sensitive data (employee liability information) directly to the transferee organisation during the process of a TUPE transfer of employees. HWD CIC (known as the Transferor) is required, in order to meet the legislative requirements of TUPE to provide, personal, contractual, statutory information directly to the new employer of its employees (known as the transferee).

5.2 The Information Commissioner's Office Data Protection Good Practice Note, Disclosure of Information under TUPE provides the following guidance:

a. What information must be given to the new employer?
b. TUPE requires that the following information (known as 'employee liability information') must be given to the new employer before the transfer takes place.
c. Identity (usually the name) and age of the employees who will transfer.
d. Information contained in their 'statements of employment particulars', such as written statement of pay, hours of work, holidays and so on (usually contained in the employee's offer letter or contract of employment).
e. Information about any relevant collective agreements.
f. Details of any disciplinary action taken against an employee in the last two years.
g. Details of any grievance action raised by an employee in the last two years.
h. Details of any legal action (before the court or employment tribunal) brought against the employer by an employee in the last two years and information about any potential legal action.

5.3 Employers must provide this information at least two weeks before the transfer is completed. If special circumstances make this impractical, employers should supply it as soon as possible.
5.4 Once the transfer is complete the transferor will provide the transferee with the HR file of the transferring employees.

6.0 **Your obligations in relation to personal information**
6.1 You must ensure that you comply with the following guidelines at all times:
a. Do not give out confidential personal information except to the data subject himself or herself. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given his or her explicit consent to this.
b. Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
c. Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
d. If you receive a request for personal information about another representative, you should forward this to HWD CIC's Data Protection Officer, who will be responsible for dealing with such requests.
e. Ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected.
f. Compliance with the Act is your responsibility. If you have any questions or concerns about the interpretation of these rules, you should take this up with HWD CIC's Data Protection Officer.
PART TWO: SERVICE USER / MEMBER OF THE PUBLIC DATA

7.0 **Data protection and client information**
The eight data protection principles apply equally to data HWD CIC holds on service users, stakeholders and members of the public. HWD CIC and all its representatives must comply with these principles at all times in their information-handling practices. In brief, the principles say that personal data must be:
a. Processed fairly and lawfully. On all occasions a person's consent will be explicitly sought for processing their data especially information relating to
- Race or ethnic origin
- Religions or other beliefs
- Physical or mental health condition
- Sexuality
- Criminal offences, both committed and alleged

b. Obtained only for one or more specified and lawful purposes in line with service specifications.
c. Adequate, relevant and not excessive. All files will be subject to file review as part of staff supervision. Reviews will ensure they do not contain out of date information and that there is sound 'case planning' reasons requiring the information to be held.
d. Accurate and up to date. File reviews will establish the accuracy of information and where appropriate and needed, seek to update.

e. Not kept longer than necessary. HWD CIC has protocols for the retention of service users' data and information. Any data HWD CIC decides it does not need to hold will be destroyed (see below).
f. Processed in accordance with HWD CIC's Confidentiality Policy.
g. Secure. Service users' files and data are confidential and are stored in locked filing cabinets. Databases and service user information held on computers must be password protected with only authorised personnel allowed access.
h. Not transferred to a country or territory outside the European Economic Area.
i. Two of the key principles of the act are particularly important in relation to the services provided by HWD CIC:

- Security
- Not kept longer than is necessary

j. The importance of the above lie in their capacity to support our commitment to the confidentiality of the service user. They help in establishing the trusting relationship so central to all HWD CIC services.
k. The following guidance exists to help all representatives better understand their responsibilities, but is not a substitute for representatives using professional judgement and acting within the spirit of the act.
l. Although these instructions are intended as HWD CIC policy or guidance, exceptions should be made in certain circumstances. HWD CIC acknowledges that some of our service users may have certain needs which mean that some of the guidance here is either inappropriate for a particular service user or that the guidance actually restricts access to the service. We do not want to be overly bureaucratic or to follow procedures just for the sake of following them. Ultimately all of this is to protect the service user so it should be up to the service user how best we do this for their particular circumstances.
m. Where a variation is to be made adequate notes should be recorded of:

- A service user's request to vary any of the usual procedures
- The reasons for this
- How HWD CIC has complied with their request and amended its procedure
- What the requested procedure is
- That a manager has been informed of this and that they have authorised it.

8.0 Electronic Documents/Communication

8.1 All individuals have a responsibility for identifying documents as confidential or restricted.
8.2 All restricted electronic documents should be labelled or watermarked as being confidential. It should also make it clear what restrictions apply to the document. For example: CONFIDENTIAL DOCUMENT – governors only.
8.3 All staff will be allocated a secure folder on their local server in which to store confidential documents.
8.4 Access to databases will be restricted to HWD CIC personnel working with the service user group.
8.5 All unattended computers shall be log-in and password protected with staff ensuring that no one, at any time, can access confidential areas of the server.
8.6 HWD CIC will increasingly be asked to communicate with service users by email and electronic mechanisms. HWD CIC must remain especially vigilant to this and ensure that

this does not accidently compromise the organisation's commitment to confidentiality and data protection.

9.0 **EMAIL**

9.1 Representatives should be mindful of the fact that emails are by default un-secure. There are methods of making emails secure – such as encryption – but as this requires special software for both the sender and the recipient it is impractical for working with service users.

9.2 There are a number of processes that representatives can go through – depending on the nature and content of the email – to ensure that they have done as much as is reasonably expected of them to get the information to the correct service user and that only they can view it.

- Ask if the service user wants to communicate by email and to what extent they want to communicate in this way – make sure that, even though they may have given their email address on first contact, they definitely want HWD CIC to use it to communicate with them. You also need to ask what HWD CIC can send them by email – letters, responses, personal details – as email addresses are not always private to that individual (e.g. work addresses)
- Ensure you have the correct email address – the email address given on first contact may not be the one that the service user wants all future communication on, so check this. Having agreed in the first step of the process how the service user wants to communicate using email then check the email has been recorded accurately.
- The service user should be told over the phone that they will sent a brief email containing no personal details. They should then reply to this email to confirm that HWD CIC are using the correct address.

9.3 Having established that the email address is correct then use it to communicate as per the service user's instructions. If the service user wants to use it simply for updates or to arrange meeting dates and times then this can be done within the body of the email.

9.4 If however the service user wants HWD CIC to send letters or other documents which are sensitive or contain personal information then we must password protect them. In particular:

- The document should be password protected to prevent it from being opened – not from being edited.
- The password should be individual for the service user but based on the same format so that another member of staff can access any files.
- The password should be told to the service user over the phone and shouldn't be sent to them in the body of any email. If the service user has asked for email correspondence only and doesn't want to talk over the phone then they should be asked how they want to receive the password. Again, if they want to opt out of this process then this is open to them but must be recorded.

9.5 Should any representative feel that this process is not suitable for a particular service user then the process can be varied provided adequate notes have been made and that it's checked with a manager.

10.0 **Telephone**

10.1 Whilst HWD CIC is not an obvious target for fraudsters it is acknowledged that the information the organisation holds on service users is often deeply sensitive and personal

and HWD CIC has a responsibility to keep it confidential to the service user (who is often a vulnerable adult or child).
10.2 Recognising the nature of the service and often the types of service users HWD CIC supports we should take a common sense and proportionate approach towards checking identity.
10.3 Situations will vary as will service users but as a minimum HWD representatives should look to confirm the identity of who is calling, their date of birth, postcode etc., to validate the caller.
10.4 Common sense will dictate that given the nature of what HWD CIC does you will only check these details if
10.4.1 This is the first time contact
10.4.2 You have spoken to them before but on this occasion you don't recognise their voice or have other doubts about their identity
10.4.3 On both occasions it should be recorded that these questions have been asked.

11.0 **Fax**
11.1 Faxing is becoming increasingly outdated but there are still instances where HWD CIC is asked to send documents or information this way.
11.2 Sensitive documents, such as medical records or letters containing medical details, must never be sent by fax, regardless of who the recipient is.
11.3 With faxing there are too many opportunities for information to go astray and to not reach its intended source. There are also better technological options such as scanning and emailing.

12.0 **Non-electronic Documents**
12.1 All non-electronic documents, for example post, must be stamped CONFIDENTIAL. It is then the intended recipient's responsibility to treat the document as confidential.
12.2 Confidential or restricted documents must always be either kept in a locked storage cabinet or within a locked room.
12.3 If kept within a locked room the room must only be accessible to those people who have the same level of access. Otherwise documents must be stored within a locked storage cabinet.
12.4 During the working day confidential or restricted documents must not be left out on desks for longer than is necessary.
12.5 At the end of a working day documents must be stored in a locked container.
12.6 Confidential or restricted documents must not be visible at any time to unauthorised members of staff, visitors or the public.
12.7 Once a confidential or restricted document is finished with it should either be filed in a secure storage container or destroyed.
12.8 Documents must be destroyed by shredding. This should be done in a timely manner in line with office protocols.

13.0 **Medical Records**
13.1 HWD CIC must not hold on to medical records, health record or medical charts for any longer than is absolutely necessary.
13.2 The terms medical record, health record, and medical chart describe the systematic documentation of a single patient's medical history and care across time within one particular

health care provider's jurisdiction. The medical record includes a variety of types of "notes" entered over time by health care professionals, recording observations and administration of drugs and therapies, orders for the administration of drugs and therapies, test results, x-rays, reports, etc.

Further information

Representatives should ensure that they read this policy in conjunction with the HWD CIC Confidentiality Policy

14.0 **Review**

This policy will be reviewed in 12 months or in the light of changes in legislation or national policy.