POLICIES AND PROCEDURES:

POLICY TITLE: DATA PROTECTION, CONFIDENTIALITY AND DATA RETENTION 2018

INTRODUCTION:

Woking Mental Health Resource Centre Ltd ("**CornerHouse**") collects and uses personal information about people who it supports, employs and works in partnership with. This information must be dealt with properly and securely however it is collected, recorded or used and this policy seeks to create safeguards to ensure all personal information is handled in accordance with the Data Protection Act 2018 (DPA) and General Data Protection Regulations 2018 (GDPR).

CornerHouse regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its functions, and to maintain confidence between those with whom it deals.

To this end **CornerHouse** fully endorses and adheres to the Principles of Data Protection, as set out in the GDPR.

The purpose of this policy is to ensure that the staff, volunteers and trustees of **CornerHouse** are clear about the purpose and principles of data protection and to ensure that it has guidelines and procedures in place which are consistently followed.

In day to day operation of the organisation, data and information can be received in a variety of ways and therefore this policy also works in conjunction with the **CornerHouse** Email and Internet Use Policy, Mobile Phone Usage Policy and a number of other policies detailed below.

Failure to adhere to the DPA or the GDPR is unlawful and could result in legal action being taken against **CornerHouse** or its staff, volunteers or trustees.

PRINCIPLES:

Both the DPA and GDPR regulate the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

To comply with the law, information must be collected and used solely for the specific purpose set out at time of collection (or with additional consent for further purposes), stored safely and not disclosed to any other person unlawfully.

To achieve this **CornerHouse** follows the seven Data Protection Principles outlined in the GDPR, which requires that personal data will be:

- processed lawfully, fairly and in a transparent manner in relation to individuals

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is absolutely necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- Accountability - the data controller shall be responsible for, and be able to demonstrate compliance with the above principles

CornerHouse employees, volunteers and trustees who process or use any personal data in the course of their duties will ensure that these principles are followed at all times.

PROCEDURES:

The following procedures have been developed in order to ensure that **CornerHouse** meets its responsibilities in terms of Data Protection. For the purposes of these procedures data collected, stored and used by **CornerHouse** falls into two broad categories:

CornerHouse's internal data records;
Staff, volunteers and trustees

CornerHouse's external data records;
Members, customers, clients.

CornerHouse as a body is a Data Controller under GDPR, and the Board of Trustees is ultimately responsible for the policy's implementation.

Internal data records:

CornerHouse obtains personal data (names, addresses, phone numbers, email addresses), application forms, and references and in some cases other documents from staff, volunteers and trustees. This data is stored and processed for the following purposes:

- Recruitment
- Equal Opportunities monitoring
- Volunteering opportunities
- To distribute relevant organisational material e.g. meeting papers

- Payroll

The contact details of staff, volunteers and trustees will only be made available to other staff, volunteers and trustees. Any other information supplied on application will be kept in a secure filing cabinet and is not accessed during the day to day running of the organisation. Contact details of staff, volunteers and trustees will not be passed on to anyone outside the organisation without their explicit consent.

A copy of staff, volunteer and trustee emergency contact details will be kept with the Business Continuity Plan for health and safety purposes to be used in emergency situations.

It is a requirement to register members of the board of Trustees and the Chief Executive with both the Charity Commission and Companies House. This includes recording personal information such as home address and date of birth. This information is not made public , however the individual will be listed under the organisations details on both websites.

CornerHouse will take reasonable steps to keep personal data up to date and accurate. Personal data will be stored for seven years after an employee, volunteer or trustee has finished working for the organisation.

Personal data is kept in paper-based systems and on a password-protected computer system. Every effort is made to ensure that paper-based data are stored in organised and secure systems.

All confidential post must be opened by the addressee only.

CornerHouse operates a clear desk policy at all times.

External data records:

CornerHouse obtains personal data (such as names, addresses, and phone numbers) from clients which is stored, and processed only for the purposes outlined in the agreement and service specification signed by the client. Information is retained solely to assist staff and volunteers in the efficient running of services and is stored electronically on the organisation's secure database and in paper form in locked filing cabinets.

During the course of supporting an individual, staff and volunteers will be party to sensitive information regarding a person's life, condition and/or treatment. Some of this information will be recorded for future reference on our secure database to assist in planning future support for the individual concerned. In all cases, staff and volunteers must respect the confidentiality of the individual and the trust placed in them through the giving of this information. *See Confidentiality and Responsibilities of Staff, Volunteers and Trustees section below.*

Individuals opt-in separately to any reminder or newsletter email services and can manage these preferences at any time.

Personal data will not be passed on to anyone outside the organisation without explicit consent from the data subject unless there is a legal duty of disclosure under other legislation. In such circumstances, the Data Officer will discuss and agree disclosure with the Chair or Vice Chair.

Only the organisation's staff, volunteers and trustees will have access to personal data. All staff, volunteers and trustees are made aware of the Data Protection Policy and their obligation not to disclose personal data to anyone who is not supposed to have it.

Information supplied is kept in a secure filing, paper and electronic system and is only accessed by those individuals involved in the delivery of the service.

Information will not be passed on to anyone outside the organisation without their explicit consent, excluding statutory bodies e.g. the Inland Revenue.

CornerHouse will take reasonable steps to keep personal data up to date and accurate. Personal data will be stored for as long as individual uses our services after which, the data we hold will be subject to our Data Retention Schedule (see below).

Enquiries:

Personal data which is collected over the phone for the purposes of an enquiry will be subject to minimal retention. The person taking the enquiry will explain the purpose of collecting the information, who and how it will be passed on and how it will be securely disposed of. It is then that individual's responsibility to carry out the data process as they have explained.

A standardised statement has been created and must be used in all circumstances that personal information is given verbally:

Under our data protection policy, the details you have given will be stored securely for the purpose of supporting you to access CornerHouse services. If you have not attended a service within 3 months from today, your information will be deleted. Please see our privacy policy on our website for more details.

In general, **CornerHouse** does not accept verbal consent for the retention or processing of personal data, except for the purpose detailed above for enquiries. Data cannot be retained further without written consent from the data subject.

CONFIDENTIALITY:

Confidentiality relates to the transmission of personal, sensitive and/or identifiable information about individuals or organisations which comes into the possession of the organisation through its work.

All personal information, whether in paper form or electronically recorded must be stored in accordance with the DPA and must be secured against unauthorised access, accidental disclosure, loss or destruction. See "Office Security" section below for further details.

CornerHouse recognises that occasions may arise where individual workers feel there us a need to breach confidentiality. Personal information relating to an individual may be divulged where there is a risk to the individual, a volunteer or employee, or a member of the public. Or in situations where is would be against the law to withhold information. In such circumstance, information may be disclosed to external agencies such as the police or social services on a need to know basis.

Where a worker feels confidentially should be breached due to a safeguarding concern, the following steps should be taken;

- The worker should raise the matter immediately with their line manager – or the most senior member of staff available. This discussion should involve an explanation on why it is felt confidentiality should be breached and what would be achieved by doing so.
- The manager will take a written note of the conversation and will be responsible for discussing available options
- The manager is ultimately responsible for deciding whether confidentiality should be breached.
- Where prior discussion is not possible, and substantial risk is imminent, the worker should refer the **CornerHouse** Safeguarding Adults Policy for guidance on how to report and record concerns.
- In such circumstances every effort should be made to inform the Safeguarding Officer or Deputy Safeguarding Officer at the earliest opportunity.

In circumstances where concerns require disclosure to other agencies it is best practice to discuss with the person concerned first, so they are aware of what is happening and in order to maintain trust between the organisation and the individual. However, this must not be done if it could lead to the individual being put at greater risk.

It is also important to note that in these situations, it is not a requirement to have the individual's consent to disclose information as concern for their welfare overrides this right.

INDIVIDUAL RIGHTS:

Under GDPR, individuals have enhanced rights in regard to their personal data. These rights include;

The right to be informed
Individuals have the right to be informed about the collection and use of their personal data. All **CornerHouse** forms which are used in the collection of information have clear details about the need for collecting information along with positive opt-in questions for joining any **CornerHouse** mailing list.

The right of access
Individuals can request access to the information held about them. This is sometimes referred to as a Subject Access Request. This is available to clients, staff and volunteers and can be requested in writing or verbally.

When a request is made, the organisation has one month to respond. Potentially any member of staff could receive this request and must pass it to the Chief Executive or most senior member of staff available immediately.

The right to rectification
Individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing.

If a request for rectification is received, CornerHouse will take reasonable steps to ensure that the data is accurate and to rectify the data if necessary. This process will consider the arguments and evidence provided by the data subject.

The right to erasure
Individuals have the right to have their personal data erased if:
- the personal data is no longer necessary for the purpose which it was originally collected or processed for
- the individual withdraws their consent to hold the information
- the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the individual objects to the processing of personal data for direct marketing purposes
- personal data has been processed unlawfully
- in order to comply with a legal obligation

The right is not absolute and only applies in certain circumstances.

The right to restrict processing
Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. Usually this would be requested as a temporary arrangement and is an alternative to erasure.

Complete information about how **CornerHouse** support these, and other rights under GDPR is maintained on the organisations website: www.cornerhouse.cc/privacy.

PRIVACY STATEMENTS:

Clear and detailed privacy notices (Appendix 1) are maintained to inform data subjects the reasons for collecting data, how it will be processed and stored and how they can access information about themselves as well as their other rights under GDPR.

These notices are available in the public domain through the **CornerHouse** website.

HANDLING DATA OFFSITE:

Information will, at times, be either collected offsite or be required to be taken to an external venue. In such circumstances, it is the individual worker's responsibility to ensure the safety and security of the information in their possession.

When required to handle information whilst aware from the main **CornerHouse** office, staff are expected to follow strict protocols at all times:

- Information should be transported directly to the office and stored securely in the relevant locked filing cabinet until further processing can take place.
- Where it is not possible to bring data directly to the office, it should be placed in a sealed, plain envelope and kept out of sight when in transit.
- Information must **never** be left unattended in a vehicle under any circumstance.

- If data is taken home (eg after an evening group offsite) then the worker must remove the information from their vehicle and store it securely. The information must be returned to the office at the absolute earliest opportunity.

Failure to adhere to these protocols will be considered misconduct and would be subject to the **CornerHouse** Disciplinary Policy.

OFFICE SECURITY:

It is vitally important that all staff remain vigilant to security at all times to protect both property and personal and confidential information held on the premises.

When away from computers these must be locked, this should occur even if a worker is only away from their computer for a short time or are the only person in the building.

Personal information must be kept in locked drawers and only accessed for specific tasks and for the minimum of time.

Offices must be locked at all times when there is no one present in the room. It is the responsibility of each member of staff to ensure they have their keys with them at all times during working hours.

Further reading: Email and Internet Usage Policy

RECRUITMENT:

Information is collected through the process of recruitment in the form of application forms, equality monitoring and occasionally CVs. All data will be kept securely and only accessed by the people involved in short listing and interviewing.

Application packs from unsuccessful candidates will be kept for seven days after notification, after which they will be securely disposed of. Data from successful candidates will be retained in their personnel file and will be subject to the Retention Schedule (Appendix 2).

Disclosure Barring Service (DBS)
CornerHouse's DBS checks are administered by Woking Borough Council (WBC) who maintain data management systems compliant with GDPR. It remains the responsibility of **CornerHouse** to ensure all outside agencies with which it shares personal information are compliant with GDPR and to act to cease sharing information with any organisation which is not compliant.

CornerHouse will not keep any photocopy or other image of DBS Certificates, Disclosure, or any copy or representation of the contents of a Disclosure or identification documents.

CornerHouse will however, 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 whether consent has been given to carry out a status check if appropriate.

Further reading: Recruitment Policy

RETENTION OF DATA:

All data obtained through the operation of the organisation is subject to the Retention Schedule (Appendix 2). This includes both electronic and physical records.

Archived documentation will be kept securely with clear details of dates to destroy. Data clean ups will be scheduled annually to ensure that documents are securely disposed of and not held for longer than is necessary.

RESPONSIBILITIES OF STAFF, VOLUNTEERS AND TRUSTEES

During the course of their duties with **CornerHouse**, staff, volunteers and trustees will be dealing with personal and confidential information and may be told or overhear sensitive information. The DPA gives specific guidance on how this information should be dealt with. In short to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. All representatives of CornerHouse must abide by this policy.

Compliance with the Act is the responsibility of all staff, paid or unpaid. **CornerHouse** will regard any unlawful breach of any provision of the Act by any member of the team as a serious matter which will result in disciplinary action. Any employee who breaches this policy statement will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Any such breach could also lead to criminal prosecution.

Any questions or concerns about the interpretation or operation of this policy statement should in the first instance be referred to the line manager.

DATA BREACHES:

Any evidence or concern of a breach of data protection must be reported to the Chief Executive, or Chair of Trustees in their absence, immediately.

Investigations will then take place to ascertain the severity of the breach, put in necessary measures to mitigate risks and to inform the people affected as well as the Information Commissioners Office. The organisation has a responsibility to report certain data breaches to the Information Commissioner Office within 72 hours, it is therefore critical that no delay occur in reporting any breaches of data.

Any member of staff found to be responsible for a data breach, whether through deliberate act or neglectful practice, will be subject to disciplinary action.

REFERENCE:

Business Continuity Plan
Disciplinary Policy
Email and Internet Use Policy
Mobile Phone Policy
Recruitment Policy
Safeguarding Adults Policy

WOKING MENTAL HEALTH RESOURCE CENTRE LTD.

Appendix 1: Privacy Notice
Appendix 2: Retention Schedule

Policy Date: 14.06.18 **Review Date: 14.06.19**

Author: Dan Curtis