DATA PROTECTION AND CONFIDENTIALITY POLICY

1. General Policy Statement

1.1 Continuum Digital Ltd is fully committed to compliance with the requirements of the Data Protection Act 1998. The organisation will therefore follow procedures that aim to ensure that all employees, and directors; along with contractors, agents, consultants, partners or others acting on its behalf; who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties and responsibilities under the Act.

1.2 Continuum Digital Ltd follows and is compliant with the General Data Protection Regulations (GDPR) 2018. All employees, and directors are trained and fully aware of the expectations and responsibilities under this guidance.

1.3 In order to operate efficiently, Continuum Digital Ltd has to collect and use information about people with whom it works. These may include members of the public; service users; current, past and prospective employees, and directors; and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used; whether it is on paper, in computer records or recorded by any other means; in accordance with the safeguards set out within this policy and the Act.

1.4 Employees, and directors may also have access to confidential information about the organisations with which Continuum Digital Ltd works and the internal business affairs of Continuum Digital Ltd , including payroll data, contracts and tenders, and other information considered 'commercially sensitive'. Access to such information is on a 'need to know' and properly authorised basis. It must only be used for the purpose(s) for which it has been authorised.

1.5 Continuum Digital Ltd regards the lawful and correct treatment of personal and/or confidential information as very important to its successful operation and to maintaining confidence between the organisation and those with whom it works. Continuum Digital Ltd will also ensure that it treats personal and confidential information lawfully and correctly.

2. Purpose

2.1 The purpose of this policy is to set out the organisation's commitment and procedures for protecting personal data and dealing with confidential information held by the organisation.

2.2 The objectives of this policy are to:

- put in place effective controls and ensure appropriate records are kept,
- meet its legal obligations under the Data Protection Act 1998 and other appropriate legislation.
- prevent inappropriate use of data held and harm to individuals whose data is held;
- meet its contractual obligations and the requirements of all parties;
- demonstrate good data protection management, respect for confidentiality and meet relevant quality assurance systems.

3. Scope

3.1 This policy applies to all employees, and directors of Continuum Digital Ltd. It also applies to all contractors, agents, consultants, partners or others acting on its behalf, who have access to any personal data or confidential information held by or on behalf of the organisation.

3.2 Continuum Digital Ltd has a range of policies and procedures, which deal with good practice standards and information processing; these include:

- Equality and Diversity
- Governance
- Financial Controls
- Recruitment
- Safeguarding
- Whistle Blowing

Employees, and directors are encouraged to use the provisions of these policies and procedures when appropriate.

4. General Principles

4.1 Continuum Digital Ltd recognises that its employees, and directors gain information about individuals and organisations during the course of their work. This may involve dealing with information such as names/addresses/telephone; as well as being told or overhearing other sensitive information about the work of Continuum Digital Ltd.

4.2 The Data Protection Act 1998 gives specific guidance on how this information should be dealt with by organisations. In essence, to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

4.3 Employees, and directors should avoid exchanging personal or confidential information or comments (gossip) about individuals and/or organisations with whom they have a professional relationship and should avoid talking about organisations or individuals in social settings.

4.4 Employees, and directors will not disclose to anyone, other than to colleagues, their line manager any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.

4.5 Employees are able to share information with their line manager/supervisor in order to share information, discuss issues and seek advice

4.6 Employees, and directors must not compromise or work to evade security measures designed to protect personal and/or confidential information.

4.7 Where there is a legal duty on Continuum Digital Ltd to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made.

4.8 Employees and directors' obligations to use and respect personal and confidential information continue to apply after they have stopped working for Continuum Digital Ltd.

5. Legislation

5.1 Information about individuals, whether on paper, in computer records or recorded by any other means; falls within the scope of the **Data Protection Act** 1998 and must comply with the data protection principles. These are that anyone processing personal data (i.e. information about identifiable, living individuals) must ensure that personal information is:

- obtained and processed fairly and lawfully;
- obtained and used only for specified purposes.
- adequate, relevant and not excessive in relation to the purpose(s) for which it is kept.
- accurate and, where necessary, kept up to date;
- not to be kept for longer than is necessary.
- processed in a way that respects the rights of data subjects.
- kept secure and protected from unauthorised or unlawful processing, accidental loss or destruction, or damage.

In addition, there are also special rules that apply to transfers abroad (including publication over the Internet).

5.2 Employees, and directors who process or use any personal information in the course of their duties must ensure that these principles are followed at all times.

6. Responsibilities

6.1 All employees, and directors; along with contractors, agents, consultants, partners or others acting on behalf of Continuum Digital Ltd are to be made fully aware of this Policy and of their duties, responsibilities and contractual obligations under the Act.

6.2 All employees, and directors will be required to sign a Confidentiality Statement before commencing work with Continuum Digital Ltd.

6.3 In relation to data protection and confidentiality issues, specific responsibilities are as follows:

6.4 Board of Directors

The Board of Directors will act as the 'Data Controller' and is the 'person' legally responsible for complying with the Data Protection Act. The Board of Directors will determine the policy, taking into account legal requirements, and ensure that it is properly implemented and adequately resourced. The Board of Directors will designate lead responsibility for data protection in the organisation to Continuum Digital Ltd.

6.5 **Data Protection Officer**

The role of 'Data Protection Officer' is delegated to the Managing Director who will be responsible for ensuring that this policy is implemented. The 'Data Protection Officer' will also have overall responsibility for:

- undertaking risk assessments and taking steps to ensure that risks are mitigated, reporting to the Managing Director and/or Board of Directors as necessary; the
- provision of data protection training for all employees and .
- the development of practice guidelines and procedures.
- advising other employees and on difficult or uncertain data protection issues. developing information sharing protocols between Continuum Digital Ltd and its
- contractors, agents, consultants, partners or others acting on its behalf.

6.6 **Managing Director**

The Managing Director will also exercise control over the following matters, in consultation and/or with the assistance of the employees of Continuum Digital Ltd:

- handling subject access requests.
- handing Freedom of Information Act requests.
- approving requests for the transfer of data to other agencies (other than established procedures already approved).
- approving unusual or controversial disclosures of personal information;
- approving information sharing protocols and contracts with data processors;
- carrying out compliance checks to ensure adherence to the Act and this policy.

7. Personal Data

7.1 The Act makes a distinction between *personal data* and *"sensitive" personal data*.

7.2 **Personal data** is defined as data relating to a living individual who can be identified from the data held and other information which is in the possession of the data controller. This includes any expression of opinion about the individual and any indication of intentions in respect of the individual.

7.3 Continuum Digital Ltd usually obtains, holds and processes the following personal data in respect of individuals:

- names;
- addresses;
- telephone numbers;
- email addresses

7.4 **Sensitive personal data** is defined as personal data consisting of information as to their:

- racial or ethnic origin;
- political opinion.

- religious or other beliefs;
- trade union membership.
- physical or mental health or condition;
- sexual life.
- criminal proceedings or convictions.

7.5 Continuum Digital Ltd may obtain, hold and process any of the above sensitive personal data in respect of individuals for specific purposes, dependent upon the area of work.

7.6 This data is obtained, stored and processed solely to assist staff within the organisation in the efficient running of the service requested by the service user or to verify a service user's feedback or evidence to research and evidence gathering.

7.7 Personal data supplied by service users is not used to send marketing material or newsletters unless permission has been granted by the service user.

8. Handling Personal and Sensitive Information

8.1 Continuum Digital Ltd will, through appropriate management and the use of

- provide and implement a Code of Practice on Data Protection and Confidentiality (as attached to this Policy).
- fully observe conditions regarding the fair collection and use of personal information.
- meet its legal obligations to specify the purpose for which information is used;
- collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- ensure the quality of information used.
- apply checks to determine the length of time information is held.
- take appropriate technical and organisational security measures to safeguard personal information.
- ensure that personal information is not transferred abroad without suitable safeguards.
- ensure that of people about whom the information is held can fully exercise the right to:
    - be informed that processing is being undertaken.
    - have access to one's personal information within the statutory 40 days.
    - prevent processing in certain circumstances.
    - correct, rectify, block or erase information regarded as wrong information.

8.2 In addition, Continuum Digital Ltd will ensure

- everyone managing and handling personal information understands that they are responsible for following good data protection practice.
- everyone managing and handling personal information is appropriately trained to do so and supervised.
- procedures are in place to respond to anyone wanting to make enquiries about handling personal information.
- queries about handling personal information are promptly and courteously dealt with.

- performance in handling personal information is regularly reviewed and evaluated.
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing.

8.3 All employees and within the organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- paper files and other records or documents containing personal/sensitive data are kept in a secure environment.
- personal data held on computers and computer systems is protected by the use of secure passwords
- contractors, agents, consultants, partners or others acting on behalf of Continuum Digital Ltd are made aware of this Policy and follow defined procedures to comply with their responsibilities under the Act.

8.4 All contractors, agents, consultants, partners or others acting on behalf of Continuum Digital Ltd will be made aware of this Policy and required to follow defined procedures to comply with their responsibilities under the Act. Any breach of the Act will be deemed as being a breach of any contract between the organisation and that individual, company, partner or firm. Independent contractors will indemnify Continuum Digital Ltd against any prosecutions, claims, proceedings, actions or payments of compensation or damages,

8.5 All contractors who are users of personal information supplied by Continuum Digital Ltd will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the organisation.

9. Monitoring and Review

9.1 This policy takes account of the Data Protection Act 1998 and other guidance available from relevant agencies.

9.2 Day to day responsibility for ensuring that the organisation keeps up to date with data protection issues and for compliance with this policy rests with the Managing Director who can also advise colleagues on any aspect of this policy.

9.3 The effectiveness of this policy, and its procedures, will be monitored and amended as and when necessary. The Managing Director may make minor changes to office procedures. Significant changes will require the approval of the Board of Directors. The policy will also be reviewed every three years as part of a continuing review of organisational policies.

DATA PROTECTION AND CONFIDENTIALITY CODE OF PRACTICE

1. Introduction

1.2 Continuum Digital Ltd is fully committed to compliance with the requirements of Data Protection Act 1998. The organisation has therefore developed a policy and this Code of Practice to ensure that all employees, and directors; along with contractors, agents, consultants, partners or others acting on its behalf; who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties and responsibilities under the Act.

2. Obtaining Personal Information by Consent

2.1 The purpose for which personal data is held varies with each area of work, each of which has clearly identified purposes related to every service user (see section 3).

2.2 When collecting personal data, it is important that we inform the data subject:

- who is collecting the data (or on whose behalf it is being collected);
- what purpose(s) the data is being collected for.
- who the data might be passed on to (and who it will not be passed to);
- how to contact us if they want to stop us from using the data or to check what we are doing with it or to change what we use the data for (for example, opting in or out of mailings or other purposes).

2.3 People being asked to supply personal data must, where appropriate, be given options on how their data will be used. This can be to opt in or opt out, for example opting in to receive mailings or the sharing of data with other organisations. They must be given a choice over direct marketing and whether their information can appear on websites. It is important that we are clear about what choices are offered, record them carefully and ensure they are acted upon.

2.4 People may also be given options on what data they provide, for example through a statement about the optional nature of a question or a 'prefer not to say' tick box when asking whether someone has a disability.

2.5 Wherever possible, written permission is sought from the service user by the use of a data protection form tailored for the area of work and/or purpose. Where written permission is not practical; the service user is informed of the purposes and verbal permission is sought.

2.6 When a referral is made via a third party (for example: a relative or friend, another service user or a partner organisation), contact must be made with the potential service user to ensure that permission has been granted to store and process their personal data.

3. Information held for Specific Purposes

3.1 The purpose for which personal data is held varies with each area of work. Those purposes are reviewed and approved by the Managing Director. Each area of work has clearly identified those purposes to every individual user.

4. Information held on Employees, and Directors for Specific Purposes

4.1 Information relating to a prospective employee's, volunteer's or director's home address, telephone numbers and email address, along with application forms, references and in some cases other details such as identity papers, qualifications and criminal records checks is held so that Continuum Digital Ltd can assess the suitability of an applicant for a specified role; set up and maintain relevant personnel records; send written communications to a home address or contact them by telephone in connection with the organisation's recruitment and selection processes and, in the case of prospective employees, meet its obligations under employment law.

4.2 Information relating to an employee's, or director's home address, telephone numbers and email address is held so that Continuum Digital Ltd can set up and maintain relevant personnel and training records, send written communications to a home address or contact them by telephone in connection with the organisation's business activities and, in the case of employees, meet its obligations under employment law or, in the case of directors, meet its obligations under company and/or charity law.

4.3 Information relating to an employee's children (up to the age of 18 years) is held so that Continuum Digital Ltd can meet its obligations for the provision of Parental Leave under the Working Time Regulations.

4.4 Information relating to an employee's home address, telephone numbers and those of designated contacts is held so that Continuum Digital Ltd can make contact with them or some other designated person in the event of an emergency (for example changes to travel arrangements or closure of business premises). In the event of the employee being taken ill, or involved in an accident or other emergency, there may be a need for the Managing Director or another member of staff to contact a friend or relative (a designated contact) of the employee or volunteer to inform them of the situation.

4.5 Information relating to an employee's home address, telephone numbers and email address is held so that colleagues can reasonably contact them at home in connection with work matters. Where a member of staff exercises an option to work at home, this data will be shared with colleagues.

4.6 Information relating to an employee's home address, personal bank account, vehicle registration, date of birth, employment and National Insurance number is held so that Continuum Digital Ltd can make arrangements to pay their salary and travel expenses. This information is also made available to our payroll services provider who will use it to make salary payments, provide the employee with a pay slip and to meet HM Revenue & Customs regulations.

4.7 Information relating to an employee's name, the job they are undertaking, relevant experience for the job, relevant qualifications and professional memberships, and business contact details is held so that Continuum Digital Ltd can release information to the public (for example business cards, emails, correspondence, organisational literature or on the website).

4.8 An employee's photograph is held, with their consent, so that Continuum Digital Ltd can use it on its website, in organisational literature and on Business / identity card).

4.9 Information about the gender, age, ethnicity, disability and employment status of employees, and directors is kept for the purposes of monitoring our Equality and Diversity Policy and may also be kept.

5. Access to Information and the Sharing of Personal Data

5.1 Work-related telephone numbers (including issued mobiles) and email addresses are freely available to all enquirers.

5.2 *Personal data*, which includes names and contact details, and *sensitive personal data* must only be shared within the organisation where necessary.

5.3 If information is issued without the necessary consent the data user must ask the Managing Director for advice.

6. Confidentiality

6.1 When printing, photocopying or working on confidential documents, data users must ensure they are not seen by people in passing. This also applies to information on computer screens.

6.2 Personal contact details, such as home and mobile telephone numbers, and emergency contacts of employees, and directors are only made available to colleagues within Continuum Digital Ltd with their explicit consent. Employees who elect to work from home must be prepared to be contacted at home by colleagues who will have access to their home and personal telephone numbers, email and home addresses.

6.3 All employees, and directors are made aware of the organisation's Confidentiality and Data Protection Policy and their obligation not to disclose personal data to anyone who is not authorised to have it. All employees, and directors will be required to sign a Confidentiality Agreement before starting work with the organisation.

7. Requests to View Records

7.1 Individual service users may request and be supplied with a copy of any personal data held by Continuum Digital Ltd by giving 21 days' notice in writing to the Managing Director. This information will be supplied free of charge.

7.2 Organisations may have sight of Continuum Digital Ltd records held in the name of their organisation. The request must be in writing from the Managing Director of the organisation concerned.

7.3 Employees may request and have sight of their personnel records by giving 14 days' notice in writing to the Managing Director.

7.4 Employees and directors may request and be supplied with a copy of all their personal data held by Continuum Digital Ltd by giving 21 days' notice in writing to the Managing Director.

8. Accuracy and Longevity of Personal Information

8.1 When recording information in case records it is important that only relevant data is recorded and that, where possible, facts are checked with the individual, a colleague or through authoritative documents. Where opinions are recorded it is important to quote the evidence on which opinions are based or to make it clear that an assumption has been made (i.e. not a checked fact).

8.2 When recording personal information in service user, organisational or personnel records it is important to ask the right questions and to explain why data is required. Systems for recording data must facilitate accurate data entry and these systems need to be synchronised regularly (where it is unavoidable to have someone's records on different systems). Data subjects must also be given the opportunity to inform us of changes to, and to check and update, their records.

8.3 Employees, and directors must inform the Managing Director of changes to their contact details so that personal data within their personnel record can be kept up to date, accurate and corrections made in a timely manner.

8.4 Employees will take reasonable steps to keep all personal data held by the organisation up to date and accurate and to make corrections in a timely manner.

8.5 Personal data relating to employees, and directors will be stored for as long as the individual is working for Continuum Digital Ltd and for five years after they have left in the case of employees and two years in the case of and directors. Once this period has elapsed, all personal data held by Continuum Digital Ltd on the individual will be destroyed.

8.6 Personal data relating to unsuccessful job applicants will be destroyed 12 months after the relevant appointment is made.

9. Security and Storage of Personal and Confidential Information

9.1 General non-confidential information about organisations is kept in filing cabinets, on bookshelves and desks, or on the computer system with open access to all Continuum Digital Ltd colleagues.

9.2 Personal information about service users and other individuals is kept in lockable filing cabinets or desks or cupboards, or on the computer system by the employee directly responsible. They must ensure that the Managing Director know how to gain access.

9.3 In order to prevent unauthorised access and accidental loss or damage to personal information held on paper, employees and should take good care of files and ring binders used in the course of their work. Where files and ring binders containing personal data or confidential information are required to be used outside of the organisation's main premises, additional care must be taken to ensure that they are not left unattended, stolen or lost.

9.4 Employees' and personnel records will be kept in a lockable filing cabinet by the Managing Director.

9.5 Financial information relating to the activities of Continuum Digital Ltd is accessible by, and is confidential to, the Managing Director, the Board of Directors and the Auditor. Financial information required by employees for the purposes of ordering goods and services

may be provided on the authority of the Managing Director. Financial information required by directors for the purposes of overseeing the organisation's finances and for authorising expenditure may be provided by the Managing Director.

9.6 Computerised records are maintained on a server in the Continuum Digital Ltd office. Where computerised records containing personal data are required to be kept on PC's or laptop computers for use outside of the organisation's office, access to computer records, networks and databases must be password protected. Employees using laptop computers for such purposes must take additional care to ensure that equipment is not left unattended, stolen or lost.

9.7 Paper records of service users' attendance at events will be kept to verify attendance. Paper records of service user feedback (e.g. user surveys, questionnaires, research etc.) may be kept for the purpose of verifying research findings. All paper records are shredded as soon as they are no longer current.

9.8 Personal data relating to employees, and directors will be stored in paper filing systems and kept in a locked filing cabinet when not in use. Contact details and birthdays will also be kept as a computerised record, which is only available to other employees. Contact details for the Managing Director may also be passed to and stored by directors.

9.9 Files containing confidential information should be labelled 'confidential'.

9.10 In an emergency situation, the Managing Director may authorise access to files by other people.

10. Duty to Disclose Information

10.1 There is a legal duty to disclose some information including:

- Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police.

10.2 In addition colleagues believing an illegal act has taken place, or that a user is at risk of harming themselves or others, must report this to the Managing Director who will report it to the appropriate authorities.

10.3 Users should be informed of this disclosure.

11. Disclosures

11.1 Continuum Digital Ltd complies fully with the Disclosure and Barring Service Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosure applications and information relating to criminal records.

11.2 Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to the Managing Director. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

11.3 Documents will be kept for as long as the individual concerned is working at Continuum Digital Ltd and then destroyed by secure means. Photocopies will not be kept. However, Continuum Digital Ltd may 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 the details of the recruitment decision taken.

12. Unlawful Disclosure of Personal Information

12.1 It is a criminal offence if anyone working for Continuum Digital Ltd discloses personal information 'knowingly or recklessly' to anyone who is not supposed to have this information. Employees and must therefore be careful if, for example, there are members of the public or staff from partner organisations in the office for any reason. They should also ensure that conversations are kept as private as possible and be aware that conversations containing personal or sensitive information may be overheard by people who should not have access to it.

12.2 Employees should also ensure that all meetings are held within specified meeting rooms and not in general office space or communal areas so as to avoid any unintentional breaches of confidentiality.

13. Use of Photographs

13.1 When taking photographs at events a notice will be displayed advising participants that photographs are being taken and that they should indicate to the photographer or the event organiser if they do not wish to be photographed.

13.2 Where practicable, Continuum Digital Ltd will seek consent of service users before displaying photographs in which they appear. A form for obtaining permission for photographs to be published can be found on the office computer network. If consent is not possible (for example a large group photo) Continuum Digital Ltd will remove any photograph if a service user or a relative/friend of the service user makes such a request. This policy also applies to photographs published on the internet.

14. Email Addresses

14.1 Outlook and Outlook Express address books are covered by the Act. Email addresses are not released without the addressee's permission. The 'BCC or blind carbon copy' facility must always be used for the bulk distribution of information to 'unspecified' email addresses.

15. Disposal of Personal and Confidential Information

15.1 Employees, and directors must be aware that names/addresses/telephone numbers and possibly details of an enquiry written on scrap paper are also considered to be confidential. Please ensure they are shredded before disposal. Similarly, information relating to financial transactions of the organisation is also considered to be confidential and should be shredded if no longer required.

16. Breach of confidentiality

16.1. Employees who are dissatisfied with the conduct or actions of other colleagues or Continuum Digital Ltd should raise this with the Managing Director using the grievance or whistle blowing procedure.

16.2. Employees, and directors accessing unauthorised files or breaching confidentially may face disciplinary action under the terms of the appropriate policy. Former employees breaching confidentiality may face legal action.

17. Further Information and Advice

17.1 Employees, and directors needing further information, advice or training on any aspect of this Policy and Code of Practice should contact Continuum Digital Ltd 's Managing Director.