Data Protection Policy

1. Statement of intent

Community Campus 87 is fully committed to compliance with its legal obligations under the General data Protection Regulations (GDPR).

The GDPR sets out how organisations keep and process data about their employees, customers, beneficiaries, suppliers and stakeholders.

This policy is in place to ensure all staff and Board Members are aware of their responsibilities and outlines how Community Campus complies with the following core principles of GDPR.

The GDPR will come into effect on 25th May 2018.

2. Legal framework

This policy has due regard to legislation including, but not limited to the following:

- The General Data Protection Regulations (GDPR)
- The Freedom from Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017), 'Overview of the General Data Protection regulation (GDPR)'
- Information Commissioner's Office (2017), 'Preparing for the General Data Protection Regulations (GDPR) 12 steps to take now'.

3. Applicable Data

For the purposes of this policy, personal data relates to an identifiable, living individual, including information such as online identifier, such as IP address. The GDPR applies to both automated personal data and to manual paper files/filing systems.

4. Principles

In accordance with the requirements outlined in the GDPR, 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 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 is 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 is processed

- 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.

5. Accountability and Responsibility

- Community Campus will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles of GDPR.
- Community Campus will provide comprehensive, clear and transparent privacy policies.
- Internal records of processing activities will include the following:

  Name and details of the organisation
  Purpose of the processing
  Description of the categories of individuals and personal data
  Retention schedules
  Categories of recipients of personal data
  Description of technical and security measures

Given the size of the organisation the appointment of a Data Protection Officer is not required under GDPR, however a GDPR team has been appointed to:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the organisations compliance with GDPR and other laws, including managing internal data protection activities, conducting internal audits and ensuring staff receive the required training.

6. Lawful Processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR data will be lawfully processed under the following conditions.

- The consent of the data subject has been obtained.
- Processing is necessary for:
  Compliance with a legal obligation.
  The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
  For the performance of a contract with the data subject or to take steps to enter into a contract
  Protecting the vital interests of a data subject or another person
  For the purposes of legitimate interests pursued by the controller or third party, except where such interests are overridden by the interests, rights of freedoms of the data subject.

7. Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific and informed and an unambiguous indication of the individuals wishes.

The organisation will ensure that individuals receive sufficient information on why their data is needed and how it will be used.

Where consent is given a record will be kept documenting how and when consent was given.

Consent can be withdrawn by the individual at any time.

8. The right to be Informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. A privacy notice must be supplied to individuals at the time of collection of personal information. It must be written in clear plain language which is concise, transparent and easily accessible.

The following information will be supplied within the privacy notice;

- The contact details of the controller and GDPR team
- The purpose of and the legal basis for processing the data
- The legitimate interests for the processing
- Any recipient or categories of recipients of the personal data
- The retention period for the personal data
- The rights available to individuals in respect of processing
- The right to withdraw consent
- Details of whether individuals are under a statutory or contractual obligation to provide the personal data
- The right to lodge a complaint with a supervising authority.

9. The right of Access

Under GDPR individuals have the right to access their personal data and supplementary information.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

Requests can be made in writing or email to the Data Controller at;

Community Campus 87 LTD
76 Brunswick Street
Stockton-On-Tees
TS18 1UU

Or via email to dpo@cc87.co.uk

We will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however we may impose a reasonable fee to comply with requests for further copies of the same information. All fees will be based on the administrative cost of providing the information.

Information will be provided without delay and within one month of date of request.

Where a request is manifestly unfounded or excessive CC87 will charge a reasonable fee or hold the right to refuse to respond to the request. In this instance the individual will, within a month, be informed of this decision, the reasoning behind it, as well as the right to complain to a supervisory authority.

10. The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties CC87 will contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort.

Requests for rectification will be responded to within one month.

Where no action is taken in response to a request for rectification, CC87 will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to Erasure

Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to offer information society services (ISS) to a child.

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- The exercise or defence of legal claims.

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

Where CC87 process the personal data of children, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent.

Where personal data has been disclosed to third parties they will be informed about the erasure of the personal data unless it is impossible or involves disproportionate effort to do so.

12. The Right to Restrict processing

Individuals have the right to block or suppress CC87's processing of personal data.

In the event that processing is restricted, CC87 will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in the future.

CC87 will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data has been disclosed to a third party CC87 will inform them about the restriction on the processing of the personal data, unless it is impossible or involves a disproportionate effort to do so.

CC87 will inform individuals when a restriction on processing has been lifted.

13. The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner without hindrance to usability.

The right to data portability only applies:

- To personal data an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract; and

- When processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine- readable form.

The information must be provided free of charge.

Where feasible, data will be transferred directly from one organisation to another organisation at the request of the individual.

CC87 will respond to any request for portability within one month.

14. The Right to Object

CC87 will inform individuals of the their right to object at the first point of communication, and this information will be outlined on the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on “grounds relating to his or her particular situation”.

CC87 must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

15. Data Security

Confidential paper records will be kept in a locked filing cabinet or drawer with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Servers containing personal information and or sensitive data will be sited in a secure location away from general office space.

Data will be backed up daily.

All servers and computers will be protected by approved security software and a firewall.

All electronic devices must be password protected which are changed regularly to protect the information on the device in case of theft.

All necessary members of staff are provided with their own secure login and password.

Data must only be saved on the organisations designated drives and servers.

If data is stored on removable media these must be securely locked away when not being used.

Data storage to mobile devices should be avoided and data must only be transferred to mobile devices if absolutely needed. The data must be deleted when finished with. The user must take every precaution to ensure the mobile device is protected from unauthorised access, theft and malicious hacking attempts and that all files are password protected.

Emails containing sensitive personal or confidential information must be password protected if there are unsecure servers between sender and recipient.

Where personal information that could be considered private or confidential is taken off CC87 premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devises under lock and key. The person taking the information from CC87 premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive it has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of CC87 premises containing sensitive information must be supervised at all times.

CC87 takes its duties under GDPR seriously and any unauthorised disclosure may result in disciplinary action.

16. Publication of Information

CC87 publishes a variety of information on its Website, including newsletters, policies and procedures, annual reports and financial information.

CC87 will not publish any personal information, including photos, on its website without the permission of the affected individual.

17. CCTV

Recording of images of identifiable individuals constitutes as processing of personal information so it is done in line with data protection principles.

CC87 notifies all staff and visitors to the premises the purpose for collecting CCTV images via notice boards and induction.

CCTV footage will be routinely kept for 28 days before being deleted.

18. **Data Retention**

Data will be retained in accordance with internal retention schedule.

Unrequired data will be deleted as soon as practicable.

19. DBS Data

All data provided by the Disclosure and Barring Service will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will not be duplicated.

And third parties who access DBS information will be made aware of the data protection legislation as well as their responsibilities as a data handler.

20. Data Breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The GDPR team will ensure that all staff members are made aware of, and understand, what constitutes as a data breach.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of CC87 becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the trust will notify those concerned directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned.

- The contact details of the DPO.

- An explanation of the likely consequences of the personal data breach.

- A description of the proposed measures to be taken to deal with the personal data breach.

- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach.