Data Protection Policy

1. Introduction

This Policy is issued in accordance with the requirements of the General Data Protection Regulations (GDRP) approved by the EU Parliament on 14 April 2016 and enforced from 25 May 2018

Sixteen sometimes enters into contracts that require it to keep and process certain information about individuals.

Sixteen also needs to keep and process information about employees and associates so that they can be recruited and paid, and legal obligations to government complied with.

To comply with the law, this information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Sixteen must comply with the GDPR which, in summary states that data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals
b) collected for specified, explicit and legitimate purposes
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
d) accurate and up to date
e) not kept for longer than is necessary

f) kept safe from unauthorised access, accidental loss or destruction.

Sixteen and all workers or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Sixteen has developed this Data Protection Policy.

2. Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees and associates will abide by the rules and policies made by Sixteen from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any person who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with the Data Controller. If the matter is not resolved, it should be raised as a formal grievance.

3. Notification of Data held and processed

All persons whose data are held by Sixteen are entitled to know

- what information Sixteen holds and processes about them and why.
- how to gain access to it.
- how to keep it up to date.
- what Sixteen is doing to comply with its obligations under the GDPR

4. Responsibilities of Employees and Associates.

Staff team members must ensure that all information that they provide to Sixteen in connection with their employment is accurate and up to date. In addition they must

- Inform Sixteen of any changes to information that they have provided, e.g. changes of address.
- If and when, as part of their responsibilities, workers collect information about other people, (e.g. as part of a service to a customer), they must comply with these guidelines.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Workers should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

5. Data Security - general staff guidelines

The personal and sensitive information collected, process and held about the individuals supported by Sixteen is the responsibility of all employees, associates and data processors. To ensure the security of data Sixteen requires that -

- The only people able to access data covered by this policy should be those who need it for their work.

- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Sixteen will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager if they are unsure about any aspect of data protection.

6 - Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to line manager, locality MANAGER OF Board member

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.

- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Personal and sensitive data must be held with the Charms Secure CMS system or password protected One Drive by Microsoft at all times.

- Data should be protected by strong passwords that are changed regularly and never shared between employees.

- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.

- Servers containing personal data should be sited in a secure location, away from general office space.

- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones except in the process of uploading to Charms CMS

- All servers and computers containing data should be protected by approved security software and a firewall.

- Any personal data that they hold electronically is kept securely, and disposed of in accordance with this policy (see Disposal of Data) at the earliest possible opportunity.

7. Rights to Access Information

All persons whose data are held by Sixteen have the right to access any personal data that are being kept about them either on computer or in certain files. Any person who wishes to exercise this right should apply to Sixteen's Locality Manager or Board Member.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing to the Sixteen's Locality Manager or Board Member.

Sixteen will make no charge for the first occasion that access is requested, but may make a charge of £10 per each subsequent request at its discretion.

Sixteen aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

8. Publication of Information

Personal contact details of employees and associates will not be made public. Some information about individual's progression into work may be made public through website, article sand social media with the express permission of the individual concerned.

9. Subject Consent

In many cases, Sixteen can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained.

Agreement to Sixteen processing some specified classes of personal data may be a condition of acceptance of some contracts. Agreement to Sixteen processing some specified classes of personal data is a condition of employment for staff or contracting work to Associates, including information about previous criminal convictions.

If fulfilment of contractual obligation requires Sixteen to ask for information about particular health needs or medical conditions:

- Sixteen will only use that information in the protection of the health and safety of the individual.
- Sixteen will need express consent to process that information therefore the individuals concerned will be asked to sign a "Consent to Process" form, regarding that type of information. A refusal to sign such a form could result in denial of service.

10. Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, ethnicity and gender and family details. This may be to ensure that Sixteen is a safe place for everyone, or to operate or monitor other policies such as Sick Pay or Equal Opportunities Policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, workers will be asked to give express consent for this. Offers of employment or Associate status may be withdrawn if an individual refuses to consent to this without good reason.

11. Designated Data Controller

Sixteen as a body corporate is the Data Controller under GDPR and the Board is therefore ultimately responsible for implementation. However, the first point of contact for enquirers, shall be Sixteen's Locality Manager or Board Member.

The Sixteen Board is responsible for ensuring that the Information Commissioners Office is properly notified and paid.

12. Retention of Data

When information is held on behalf of customers, Sixteen will abide by the customers' requirements for the retention of that information.

In other cases Sixteen will retain data for the period required to ensure that it complies with law such as employment law, or where it is essential to provide a service to clients.

Data will be archived 6 months after an individual service is completed unless ongoing employment monitoring is requested.

13. Disposal of Data

When personal data is no longer required, or has passed its retention date, paper records must be shredded. If there is a significant amount of material which cannot be dealt with using normal shredding machines; this should be disposed of using a reputable disposal contractor.

Charms data will be archived buy may be used for statistical purposes.

14. Compliance Requirements

Compliance with the GDPR is the responsibility of all Sixteen employees and associates. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Data Controller.

Agreed at Sixteen …….. Meeting on …….. [date]