The Council has adopted a policy which h

Data

Protection

Policy

The Big Fresh Catering Company

December 2019

**Index**

**Page**

**1. Introduction ……………………………………………………………………………** 2

**2. Governance and Accountability …………………………………………………...** 2

**3. Definitions ……………………………………………………………………………..** 3

**4. Data Protection Principles ………………………………………………………….** 3

**5. Legal Basis for Processing …………………………………………………………** 4

**6. Individual Rights ……………………………………………………………………...** 5

**7. Privacy Notices ………………………………………………………………………..** 6

**8. Right to Rectification and Erasure …………………………………………………** 6

**9. Records Management ………………………………………………………………..** 6

**10. Security ………………………………………………………………………………..** 6

**11. Contracts / Data Sharing …………………………………………………………...** 7

**12. Data Protection Impact Assessment (DPIA) ……………………………………** 7

**13. Data Breaches ………………………………………………………………………..** 8

**14. Compliance Status …………………………………………………………………..** 8

**DATA PROTECTION POLICY**

**1. Introduction**

This policy outlines how the Big Fresh Catering Company will comply with its

responsibilities under the General Data Protection Regulations and the Data Protection Act 2018, current guidance and other related data protection legislation.

This policy is supplemental to other policies in respect of information management.

The Big Fresh Catering Company needs to collect and use certain types of personal information to operate effectively. This includes information on current, past and prospective employees, suppliers, clients / customers, residents, tenants, partners and others with whom it communicates. This personal information must be dealt with properly no matter how it is collected, recorded and used – whether on paper, by computer or recorded on other material.

**2. Governance and Accountability**

All staff have responsibilities for ensuring the security and safekeeping of the

Big Fresh Catering Company’s Information as set out in the Employees’ Information Security Responsibilities Document, the ICT Code of Conduct and any other supplemental guidance issued.

Appropriate training including E-training will be provided to all staff processing

personal data. All staff processing personal information are required to attend such

training.

Managing Director responsibilities are set out within The Big Fresh Catering Company’s Financial Procedure Rules, contained in The Big Fresh Catering Company’s Constitution.

Day to day responsibility for ensuring the implementation of this policy will operate

under the auspices of The Big Fresh Catering Company’s Shareholder Committee, which in turn will be supported by the Board of Directors.

Overall responsibility for data protection has been delegated to the Managing Director.

A record of internal processing activities will be maintained. Clear, comprehensive

and transparent privacy policies and procedures will be maintained. All staff are

required to adhere to the requirements, which are available to staff within the policy folder on Cypad.

**3. Definitions**

There are two classes of personal data,

*‘Personal Data’ -* any information relating to an identifiable person who can be

directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal

data, including name, identification number, location data or online identifier,

reflecting changes in technology and the way organisations collect information about

people.

*‘Sensitive personal data’* – Article 9 of the GDPR refers to sensitive personal data as

“special categories of personal data”. Personal data revealing racial or ethnic origin,

political opinions, religious or philosophical beliefs, or trade union membership, and

the processing of genetic data, biometric data for the purpose of uniquely identifying

a natural person, data concerning health or data concerning a natural person’s sex

life or sexual orientation.

4. **Data Protection Principles**

The Big Fresh Catering Company regards the lawful and proper treatment of personal information as being fundamental to the effective delivery of its objectives and is key to the maintenance and confidence between The Big Fresh Catering Company and its customers and employees.

Under the GDPR, the data protection principles set out the main responsibilities for

organisations.

Article 5 of the GDPR requires that personal data shall be:

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

b) collected for specified, explicit and legitimate purposes and not further processed

in a manner that is incompatible with those purposes; further processing for archiving

purposes in the public interest, scientific or historical research purposes or statistical

purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for

which they are processed;

d) 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;

e) 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; and

f) 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.”

Article 5(2) requires that:

The controller shall be responsible for, and be able to demonstrate, compliance with

the principles.

All personal data will be processed in accordance with the principles and by

reference to the latest guidance produced by the Information Commissioner’s Office,

the Welsh Local Government Association and other relevant bodies, and in

accordance with recognised good practice.

**5. Lawful Basis for Processing**

Personal information will only be processed where there is a lawful basis for doing

so. There are six available lawful bases for processing. Which basis is most

appropriate to use will depend on your purpose and relationship with the individual.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of

these must apply whenever you process personal data:

(a) **Consent**: the individual has given clear consent for you to process their personal

data for a specific purpose.

(b) **Contract**: the processing is necessary for a contract you have with the individual,

or because they have asked you to take specific steps before entering into a

contract.

(c) **Legal obligation**: the processing is necessary for you to comply with the law (not

including contractual obligations).

(d) **Vital interests**: the processing is necessary to protect someone’s life.

(e) **Public task**: the processing is necessary for you to perform a task in the public

interest or for your official functions, and the task or function has a clear basis in law.

In order to lawfully process sensitive personal data, you must identify both a lawful

basis under Article 6 and a separate condition for processing special category data

under Article 9. These do not have to be linked.

This document acts as the Policy Document in compliance with paragraph 30 of

Schedule 1, Part 4 of the Data Protection Bill. The Controller’s procedures will be

set out in relevant guidance procedures and training to staff, to comply with

paragraph (a). The Controller’s Retention Policies are as set out in the Retention

Schedule to comply with paragraph (b).

**6. Individual Rights**

The Big Fresh Catering Company regards individuals’ rights as fundamental to its customers and staff and therefore endorses the enhancement of individual data rights as set out in the legislation. All requests for personal information will be dealt with in accordance with the individual’s statutory rights. Queries regarding The Big Fresh Catering Company’s processing of personal data will be dealt with promptly and courteously.

The GDPR provides the following rights for individuals:

1. The right to be informed

2. The right of access

3. The right to rectification

4. The right to erase

5. The right to restrict processing

6. The right to data portability

7. The right to object

8. Rights in relation to automated decision-making and profiling.

**Children’s Rights**

The GDPR contains new provisions intended to enhance the protection of children’s

personal data. Where services are offered directly to a child, organisations must

ensure that the privacy notice is written in a clear, plain way a child understands.

**7. Privacy Notices**

The Big Fresh Catering Company will, at the point of collection, unless an appropriate exemption applies, inform individuals of the specific purpose or purposes for which The Big Fresh Catering Company will use personal information. To ensure the information required by Article 13 is communicated to the individual, The Big Fresh Catering Company will use a layered approach for Privacy Notices.

**8. Right to Rectification and Erasure**

The GDPR gives individuals the right to have personal data rectified if it is inaccurate

or incomplete. The Big Fresh Catering Company will make it easy for individuals to access and correct their personal information. Where a request for rectification is received, the statutory time limit is one month. This can be extended by two months where the request for rectification is complex.

The right to erasure is also known as “the right to be forgotten” and enables an

individual to request the deletion or removal of personal data where there is no

compelling reason for its continued processing. There are some specific

circumstances where the right to erasure does not apply.

**9. Records Management**

Personal information will be held for the duration specified in The Big Fresh Catering Company’s retention schedule. All staff will be expected to comply with the Lord Chancellor’s Code of Practice for Record Management.

**10. Security**

The GDPR requires personal data to be processed in a manner that ensures its

security. This includes protection against unauthorised or unlawful processing and

against accidental loss, destruction or damage.

Appropriate technical and organisational measures will be taken to ensure the

security of such data and including:

The pseudonymisation and encryption of personal data;

The ability to ensure the ongoing confidentiality, integrity, availability and resilience

of processing systems and services;

The ability to restore the availability and access to personal data in a timely manner

in the event of a physical or technical incident;

The regular testing, assessing and evaluating the effectiveness of technical and

Organisational measures for ensuring the security of the processing.

All staff (including agency staff) processing personal information on The Big Fresh Catering Company’s behalf will be appropriately trained.

Access to personal information will be strictly controlled through the use of password

and encryption facilities. Access to systems will be restricted to those users that

need it to undertake their duties, access rights will be reviewed on a regular basis.

Security measures will be implemented to ensure that personal information is not

automatically made widely available.

The Big Fresh Catering Company has developed a comprehensive set of procedures and guidance to comply with this requirement. All members of staff are required to comply those provisions.

**11. Contracts / Data Sharing**

When third parties handle data on behalf of The Big Fresh Catering Company such as contractors, agents, partners, consultants, etc. there will be a written agreement between The Big Fresh Catering Company and the third party confirming that they have appropriate technical and organisational security measures in place to safeguard the personal data and such third parties will only act on the instructions of The Big Fresh Catering Company. The Big Fresh Catering Company will comply with the requirements for third party processing as set out in Article 28 of the GDPR. The Big Fresh Catering Company will only appoint contractors who can provide “sufficient guarantees” that the requirements of the GDPR will be met and the rights of individuals are protected.

**12. Data Protection Impact Assessment (DPIA)**

Data protection impact assessments are a tool which can help identify the most

effective way to comply with their data protection obligations and meet individuals’

expectations of privacy. An effective DPIA will allow you to identify and fix problems

at an early stage, reducing the associated costs and damage to reputation, which

might otherwise occur.

Officers must carry out a DPIA when:

• using new technologies; and

• the processing is likely to result in a high risk to the rights and freedoms of

individuals.

**13. Data Breaches**

The GDPR introduced a duty on all organisations to report certain types of data

breach to the Information Commissioner’s Office.

A personal data breach means a breach of security leading to the destruction, loss,

alteration, unauthorised disclosure of, or access to, personal data. This means that

a breach is more than just losing personal data, for example, unauthorised access is

also a breach.

The Big Fresh Catering Company has 72 hours from the time they become aware of it, to report the breach to the Information Commissioner’s Office, if appropriate.

**14. Compliance Status**

Compliance with this policy and the guidance for managers is mandatory. Breach of

this policy by The Big Fresh Catering Company’s employees will be regarded as gross misconduct and may lead to termination of employment.