Title	HR608B - IT Data Confidentiality Storage Security Data Protection Policy	Importance	A - Critical
Document Type	Policy	Version	8.0
Page	1	Owner	SMT

IT & Data Confidentiality, Storage, Security & General Data Protection Policy

PURPOSE
The purpose of this policy is to set out the obligations and expectations of all individuals who should use and or be affected by this Policy, supplementary policies, and related legislation.

SCOPE
This policy applies to those authorised persons working with or for The Food and Drink Forum or for those persons authorised and requiring to be on the premises to which the Food and Drink Forum operate i.e. all directors, staff, subcontractors, third party agents, clients and visitors who may access, use, handle or manage information, services, facilities or activities. It is acknowledged that some policies may have more application to one group than others. This policy should also be read in line with related and or associated policies.

AIM
The aim of this policy is to create a positive working environment by which everyone understands the expectations of themselves and each other and to enable all employees to fully appreciate the Company policy on the matter, procedures to be followed and consequences of non-compliance which may lead to disciplinary action being taken up to and including dismissal.

Approach
Our employee data policies outline our guidelines for; using our company's internet connections, IT infrastructure, network and equipment; maintaining and responsibilities for confidentiality; the safe storage of and the preserving of the security of our data and that of client and employee information and sensitive data together with the usage and restrictions in accordance with the General Data Protection Regulations (GDPR).
The General Data Protection Regulation (GDPR) Policy 2018 supersedes the Data Protection Act 1998 (directive 95/46/EC) with effect from 25th May 2018, affecting all UK companies who process or store personal information.

The GDPR policy is focused on looking after the privacy and rights of the individual, and based on the premise that consumers and data subjects should have knowledge of what data is held about them, how it's held, and other core information that the Data Protection Act did not originally demand. Whilst it's designed to strengthen and unify data protection for individuals within the European Union, it also deals with the export of personal data outside the EU too. A Privacy Policy is internally focused, telling employees what they may do with personal information, while a privacy notice is externally facing, telling customers, regulators and other stakeholders what the organisation does with personal information.

The more we rely on technology to communicate, collect, print, store and manage information, the more vulnerable we become to severe security breaches. Human error, negligence and or ignorance, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation. We want to avoid inappropriate or illegal IT and data use that creates risks for our company's legality and reputation. For this reason, we have implemented a number of measures,

guidance, policies and procedures that may help mitigate risks and have provided provisions in this policy.

The purpose of this policy is to outline essential roles and responsibilities within the Food and Drink Forum for creating and maintaining an environment that safeguards data from threats to personal and professional interests and to establish a comprehensive data usage and storage program in compliance with applicable laws and in line with applicable quality standards. This policy is also designed to establish processes for ensuring the appropriate usage, security and confidentiality of confidential and sensitive information and to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information. The policy is also to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

In the event that any particular information at the Food and Drink Forum is governed by more specific requirements under other policies or procedures the more specific requirements shall take precedence over this policy to the extent there is any conflict.

The Forum will choose a third party IT supplier for IT support, storage and security of systems (currently Central Technology Limited or other third party). Any third party supplier must be accredited against the quality standards 27001 to ensure the safety of the Forums data and that of any client in addition Data Protection Policies which comply with the relevant Act.
This policy applies to all Food and Drink Forum staff, whether full or part-time, paid or unpaid, temporary or permanent. This policy applies to all information accessed, collected, stored either electronically or hard copy, or used by or on behalf of any operational team, projects and persons within Food and Drink Forum operations, including stakeholders, volunteers, sub-contractors, third parties or clients and visitors. In the event that any particular information at the Food and Drink Forum is governed by more specific requirements under other policies or procedures the more specific requirements shall take precedence over this policy to the extent there is any conflict. This Policy combines the Food and Drink Forum's rules and Government Legislation in relation to information technology and data usage in areas of;

A. IT Usage – Policy Elements
B. IT Security – Policy Elements
C. Confidentiality - Policy Element
D. General Data Protection Regulations (GDPR) 2018 – Policy Elements
E. Policy Declaration

Implementation of the Policy

The Food and Drink Forum has an IT Administrative Representative who will be responsible for the management of the system, together with the General Manager. This person will be available for advice on all aspects of the policy.
All incoming and outgoing e-mail and Internet access is logged. These logs are subject to regular review, carried out by the General Manager. Hard copies of e-mail messages may be used as evidence in disciplinary proceedings.
Access to all the Food and Drink Forum's systems (including e-mail and Internet) is controlled through a system of user identifications and passwords. All users are issued with a unique individual password,

which must be changed at regular intervals and is confidential to the user. Disclosing a password to any other employee is likely to result in disciplinary action, including summary dismissal. Should a circumstance arise where it is necessary for an employee to access a system using another employee's credentials, then authorisation must be sought from the General Manager who will instruct the IT Administrative Representative to grant such access.

Users must ensure that critical information is not stored solely within the e-mail system. Hard copies must be kept or stored separately on the system. If necessary, documents must be password protected.

Users are required to be familiar with the requirements of updated data protection legislation and to ensure that they operate in accordance with the requirements of the Act.
Employees who believe they have cause for complaint as a result of e-mail communications should raise the matter initially with their Line Manager and/or the IT Representative. If necessary, the complaint can then be raised through the Grievance policy.

Ensuring the Effectiveness of the Policy
All Board members will receive a copy of this policy. Existing and new workers will be introduced to the confidentiality policy via induction and training. The policy will be reviewed annually and amendments will be agreed by the General Manager.

Non-adherence
Breaches of this policy or any element within will be dealt with under the Grievance and/or Disciplinary procedures and or following criminal proceedings as appropriate.

A. <u>IT Usage - Policy Elements</u>
This Policy is designed to protect both The Forum and its employees from:
- Unauthorised persons accessing the system and data.
- The corruption of data either inadvertently or maliciously.
- Loss of data from system failure.
- Human error or negligence
- Virus attacks.

And to provide guidelines on the use of equipment and applications including;
- Company e-mail
- Internet

Company-issued equipment
1. We expect our employees to respect and protect our company's equipment. "Company equipment" in this policy for employees includes company-issued phones, computers, laptops, tablets and any other electronic equipment belonging to our company.
2. All work should be used via the 'cloud' as provided by Central Technology (or other third party IT provider from time to time) as this is a secure environment.
3. We advise our employees to lock their devices in their desks/cabinets when they're not using them. Our employees are responsible for their equipment whenever they take it out of the office.

4. The computer is for your usage only. Under no circumstances should any family member or other person be allowed to use it. It is for business use only. Limited personal use outside of working hours may be acceptable if authorised by the General Manager.
5. The PC/laptop and all software loaded on it remain the sole property of the Food and Drink Forum or third party provider and must not be changed, altered or disassembled in any way. Under no circumstances should any other software or applications be downloaded on to the computer unless with specific permission from the General Manager.
6. Please ensure that all computer equipment, software, and data are protected from potential damage however caused.
7. The computer should never be left unattended with information on the screen that could be viewed by another person. All data is private and confidential and must only be used for Food and Drink Forum business. If computers are to be left unattended users must log off the system.
8. Laptop computers should never be left on open view in a car. Always lock them in the boot if you are leaving the vehicle and always take them into your home at night.
9. It is recommended that you do not carry your laptop in a computer case as this is an obvious risk of theft. You will be given an allowance to purchase a holdall of your choice and it is recommended that you use a wheelie case at all times, especially when entering and leaving the Food and Drink Forum offices or client site.
10. All work must be saved on the network drives (cloud) and not on desktops or stored on the PC/Laptop drives. However, if approved and required to work off the cloud then you must make sure that your PC/Laptop is regularly backed up (weekly minimum for office workers) and secure.
11. Decisions regarding changes to the IT system in any way whatsoever must first be discussed with the General Manager.

Use of e-mail, Internet and Equipment

The e-mail system and the Internet are available for communication on matters directly concerned with the business of the Food and Drink Forum. Personal use of e-mail and the Internet on the Food and Drink Forum's system is limited to outside of working hours or as agreed by the General Manager. Employees using the e-mail system should give particular attention to the following points:

1. **Emails:**
2. The standard of presentation. The style and content of an e-mail message must be consistent with the standards that the Food and Drink Forum expects from written communications, i.e. courteous, polite and helpful.
3. The extent of circulation. E-mail messages should only be sent to those employees or clients for whom they are particularly relevant.
4. The appropriateness of e-mail. E-mail should not be used as a substitute for face-to-face communication.
5. Abusive e-mails can be a source of stress and can damage work relationships. Hasty messages, sent without proper consideration, can cause unnecessary misunderstandings.
6. The visibility of e-mail. If the message is confidential, the user must ensure that the necessary steps are taken to protect confidentiality. The Food and Drink Forum will be liable for any defamatory material of unauthorised disclosure of confidential information circulated either within the Food and Drink Forum or to external users of the system. To lessen the risk of

unauthorised disclosure, all e-mails to external users should contain the message at paragraph 7 below or updated version.

7. E-mail contracts. Offers or contracts transmitted via e-mail are as legally binding on the Food and Drink Forum as those sent on paper. Care must therefore be taken not to create a binding contract by anything sent by e-mail. For this reason, all e-mails to external sources should include the statement set out in paragraph 7 below.
8. All e-mails to external users should contain the following as defined and issued by the Systems Administrator:

9. ***"The information in this e-mail and any attachments or any reproduction of this e-mail in whatever manner is confidential and for the use of the addressee(s) only. If you are not the addressee then the distribution, use or reproduction of this e-mail or the information within it is strictly prohibited and may be unlawful. If received in error please advise the sender and delete all record of it from your system. Although believed to be virus free, accurate and complete, responsibility for any loss or cost arising from its receipt or use or its incomplete or inaccurate transmission is hereby excluded to the fullest extent possible. The views expressed by the individual in this email are not necessarily those held by The Food and Drink Forum Nothing in this e-mail is intended to constitute a binding offer or contract and there is no intention on the part of the sender, whether on his own behalf or on behalf of any other person, by this e-mail to enter legal relations with you or any other person."***
10. An employee who uses the internet or internet e-mail shall:
11. Be responsible for the content of all text, audio, or images that he/she places or sends over the internet.
12. All communications should have the employee's name attached.
13. Immediately delete any personal emails received with attachments requiring downloading or of an unacceptable nature and advise their manager accordingly. They should also advise those sending this type of information that they are not available to receive data of this nature at their workplace
14. The email system must not be used to send illegal or any material that could be considered to be obscene or offensive.
15. You must not knowingly transmit any viruses or malicious code.
16. Remember there is no such thing as private e-mail; the recipient may forward it on.
17. Be conscious that the following are regarded as particularly serious and may be regarded as gross misconduct:
18. Any message that could constitute bullying or harassment. What matters is how it affects the recipient, so thoughtlessness or "just a bit of fun" is no defence
19. Excessive or unnecessary personal use, e.g. social invitations, jokes, cartoons or chain letters.
20. Conducting a personal business using company resources
21. on line gambling
22. accessing pornography
23. downloading or distributing copyright information and/or any software available to the user
24. posting confidential and/or personal information about other employees, the Food and Drink Forum or its clients or suppliers
25. circulation of unsolicited e-mail
26. responding to chain e-mails
27. issuing warnings about viruses and potentially spreading a virus knowingly or not

28. **Internet:**
29. Access is provided as part of a standard logon, staff are therefore responsible for all Internet usage.
30. Bear in mind health and safety: VDU regulations of no more than 45 to 60 minutes of usage at a time, control staff use especially when using the Internet as it can be addictive.
31. Any irregularities in the use of the Internet through monitoring will be reported to the General Manager. All staff usage will be monitored and any access to inappropriate or explicit material will be reported directly to the Managing Director.
32. Ensure any purchases over the Internet are covered by a purchase order/contract signed and authorised by a budgetary authority as if staff were handling a manual transaction.
33. Before entering any private information relating to The Forum including credit cards, ensure staff are on a secured site (noted by a padlock in the top bar/site address) and check any fraud policy.
34. Personal use of the Internet is only permitted with request and authorisation from the General Manager in accordance with this policy and in staff own time (i.e. lunch time and after working hours).

35. **Equipment:**
36. Not connect any other computer or device to the network without prior approval of the IT support.
37. Note specific on-line services (other than the Internet) that require connection to an external source must be approved by the General Manager to ensure security.
38. Not load any personal software or attach external devices without prior consent of the General Manager.
39. Contact the General Manager if requiring to purchase (via a purchase order form) or relocate any computer related items.
40. Avoid placing storage media near devices emitting strong electromagnetic fields (mobile phones, cordless phones, loud speakers, monitors/VDUs) or direct sunlight.
41. Avoid smoking, eating or drinking near computer equipment.
42. Not copy any The Forum data or software programs.
43. Not personally load programs on to The Forum computer systems. Request for programs to be loaded should be made to the General Manager who will ensure that valid licenses are held to prevent unauthorised software being loaded.
44. Note staff password must be given to the General Manager for safekeeping.
45. In the case of a Forum computer equipment being lost or stolen, then The Forum should pay for the replacement. However, staff should be aware that they will be expected to cover the cost if they have been negligent, i.e. leaving a laptop on plain view in an unlocked vehicle etc.
46. All laptops/notebooks are to be password protected in case the laptop/notebook is lost to prevent leakage of data with the password given to the General Manager.

Viruses:

Computer Viruses can cause serious damage to the Food and Drink Forum's computer system and in some cases could be catastrophic. It is vitally important that you comply with all instructions from our IT Administrative Representative to prevent viruses entering or damaging the system.

Attachments to or links within general e-mails **must not** be opened without firstly considering whether you are expecting it, secondly review in detail the email address it was sent from i.e. spam/virus emails

look similar but may be slightly different fay.davies@online.foodanddrinkforum.co.uk or check with our IT Administrative Representative first even if the source of the e-mail is known and it is known to be reliable. Here spam/viruses are a possibility, inform the actual person where the potential/suspect email had come from stating that their email may have been compromised.
Any discs used from a source other than the Food and Drink Forum must be checked for viruses first by our IT Administrative Representative.
If you receive a warning about a virus DO NOT E-MAIL the warning to everyone in the Food and Drink Forum – that will clog up the system, which is precisely what the virus itself aims to do. Most virus warnings are hoaxes unless they come from an authoritative source. If a virus warning is received, contact our IT Administrative Representative and Central Technology (or other third party IT hosts from time to time) who will check on the authenticity of the warning and whether any action need be taken.

Downloads:
File downloads from the internet are not permitted unless for work related activity and from a reputable site or as specifically authorised in writing by the IT Administrative Representative or General Manager. There should be no downloads whatsoever in terms of music, personal pictures and or games. If downloading information, be aware that files may:

1. Contain viruses
2. Be subject to copyright law
3. Be subject to licensing agreements

Interception of Communications
The Food and Drink Forum reserves the right to monitor, intercept and read any internal or external email or fax or to listen to or record any telephone conversation for the purposes of **monitoring** and record keeping to establish; facts, compliance with regulatory or self-regulatory procedures, to prevent or detect crime, to investigate or detect the unauthorised use of the Food and Drink Forum's telecommunication system or to ascertain compliance with the Food and Drink Forum's practices or procedures. The Food and Drink Forum may also monitor, intercept, read, listen or record communications to check whether communications are relevant to the business. The Food and Drink Forum also reserves the right to monitor Internet usage to check compliance with section 6 above.

The Food and Drink Forum does not routinely monitor employees' use of the Internet or the content of email messages sent or received. However, the Food and Drink Forum has a right to protect the security of its systems, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon it. To achieve these objectives, the Food and Drink Forum carries out random spot checks on the system which may include accessing individual email messages or checking on specific Internet sites that have been accessed. The Food and Drink Forum also reserves the right to read employees' emails to check for business emails whilst they are absent or out of the office. The Food and Drink Forum may also access employees' voicemail to check for business calls whilst they are absent or out of the office. It may therefore be unavoidable that some personal messages will be read or heard.

Passwords
Passwords are the most effective measure against unauthorised access to a system. Company passwords only are to be used unless authorised otherwise. Entry to systems is usually caused by bad

passwords, which are easy for a potential intruder to guess. If authorised to use a password other than a company one, some suggestions/tips for selecting good passwords are:

1. Don't use staff login name
2. Don't use personal information such as name, address, phone number, date of birth, NI number, job title, vehicle license plate number etc.
3. Don't use keyboard sequences. i.e. qwerty, zxcvb
4. Don't use any of the above spelt backwards
5. Avoid using 'all numeric' or all text passwords
6. Don't use sample passwords from security texts
7. Do use at least six characters
8. Do use a mix of numbers and mixed case letters
9. Do use a seemingly random selection of letters and numbers
10. Liaise with the IT Administrative Representative in relation to local passwords

Staff passwords are personal:

1. Do not share it with anybody else
2. Do not write it down
3. Challenge anybody who appears to be using an unauthorised password
4. Report any misuse to the General Manager or IT administrative Representative

Employees with Administrator Access

This policy element is an extension to the Food and Drink Forum's confidentiality policy element and applies only to those persons who have administrative access rights to any of the Companies IT, network and / or server system ("administrator"); Responsibilities of Administrators are;

- The administrator/s should keep passwords secure and not pass on to anyone without the permission of the IT Administrative Representative. If you think that password has been compromised, you should immediately inform the IT Administrative Representative who will arrange for it to be changed.
- All information contained on any IT file, database, network drive, server, and the method of accessing it, other than information held in public folders, is confidential, and should only be accessed by the administrator with the permission of the person to whom it relates, or the General Manager.
- As administrator, your duties are to ensure the smooth day to day running of the Forum's IT, data, filing systems, network and server. This will sometimes necessitate changing settings, adding and removing users, and responding to queries and problems encountered by the users. The method of making these changes must not be made known to anyone who has not been granted administrator rights, and changes should only be made when necessary.
- It may sometimes be necessary for the Food and Drink Forum or one of the administrators to make changes remotely. The other administrators will always be informed of these changes as soon as possible.
- Any problems that are encountered that are outside the capabilities of any available internal IT administrator should always be referred to Central Technology Limited
- The administrators must not make any changes to any systems that are not crucial to the smooth running of the network and server.
- Employees and employees with administrative rights are bound by the Confidentiality Policy element and the General Data Protection Regulations Policy in addition to any legislative changes and agreement signed.

Data Protection
A simple rule – we can only give data to third parties that are doing work for or in conjunction with The Forum. Should this be the case a signed letter will be required saying they are using the data for the specific function required by The Forum and will not use, distribute or divulge the information to any other parties. A copy of the letter needs to be filed with the IT Administrative Representative. The General Manager must authorise any data transfer prior to any agreement.

B. <u>Data Security - Policy Elements</u>

Confidential data **is secret and valuable. Common examples are:**

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Definitions
Information Resource. An Information Resource is a discrete body of information created, collected and stored in connection with the operation and management of the Food and Drink Forum and used by employees of the Food and Drink Forum having authorised access as a primary source. Information Resources include electronic databases as well as physical files. Information derived from an Information Resource by authorised users is not an Information Resource, although such information shall be subject to this policy.

- Sponsors. Sponsors are those staff of the Food and Drink Forum that have primary responsibility for maintaining any particular Information Resource.
- Users. Users include virtually all Food and Drink Forum staff to the extent they have authorised access to Food and Drink Forum Information Resources, and may include students, faculty, staff, contractors, consultants and temporary employees and volunteers.
- 'Personal **data**' means **data** relating to a person who can be identified from it (either on its own or from a combination of that data and other data held by the Data Controller or likely to come into his possession). This includes expression of opinion about the person and any indication of someone else's intentions towards him.
- 'Sensitive personal data' means personal data about someone's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sexual life, actual or alleged commission of any offence, or any court proceedings relating to such an offence or its outcome
- 'Processing' of data means obtaining, recording, holding or doing anything with it, such as organising, altering, retrieving, disclosing or deleting it.

Data Classification
All information covered by this policy is to be classified within one of three categories, according to the level of security required. In descending order of sensitivity, these categories (or "security classifications") are "Confidential," "Internal Use Only," and "Public."

- Confidential information includes sensitive information, and must be given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access or modification to confidential information may result in direct, materially negative impacts on the finances, operations, or reputation of the Food and Drink Forum.
- Internal Use Only information includes information that is less sensitive than confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of the Food and Drink Forum.
- Public information is information that is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on the Food and Drink Forum or upon the finances, operations, or reputation of the Food and Drink Forum.

All Information Resources, whether physical documents, electronic databases, or other collections of information, are to be assigned to a security classification level according to the most sensitive content contained therein. Where practicable, all data is to be explicitly classified, such that Users of any particular data derived from an Information Resource are aware of its classification.

In the event information is not explicitly classified, it is to be treated as follows: Any data which includes any personal information concerning a member of the Food and Drink Forum shall be treated as Confidential. Other information is to be treated as Internal Use Only, unless such information appears in form accessible to the public (i.e., on a public website or a widely distributed publication) or is created for a public purpose.

Security Responsibilities

- It is the policy of the Food and Drink Forum that all confidential and other sensitive information be safeguarded from unauthorized access, use, modification or destruction. All employees of the Food and Drink Forum share in the responsibility for protecting the confidentiality and security of data.
- Sponsors. A Sponsor has primary responsibility for overseeing the collection, storage, use and security of a particular Information Resource

  A Sponsor is responsible for the following specific tasks associated with the security of the information:
  - Ensuring that the Information Resource is assigned a security classification and that such data is marked where appropriate.
  - Identifying authorised Users of the Information Resource, whether by individual identification of by job title.

Enforcement Sanctions

The Food and Drink Forum reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this policy. Violations of this policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this policy may result in dismissal from the Food and Drink Forum.

The Food and Drink Forum maintains a computer security system that provides at a minimum to the extent technically feasible:

- Secure user authentication protocols including:

  - control of user IDs and other identifiers;
  - a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
  - control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
  - restricting access to active Users and active User accounts only; and
  - blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.
- Secure access control measures that:
  - restrict access to records and files containing Confidential information to those who need such information to perform their job duties; and
  - assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access that are reasonably designed to maintain the integrity of the security of the access controls.
- Encryption of all transmitted records and files that will travel across public networks, and encryption of all data to be transmitted wirelessly.
- Reasonable monitoring of systems.
- Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
- Education and training of employees on the proper use of the computer security system and the importance of data security.

C. <u>Confidentiality – Policy Elements</u>

The Forum is committed to providing a confidential service to its employees, directors, sub-contractors, users, clients, visitors and stakeholders. No information given to the company or its employees will be shared with any other organisation or individual without the user's expressed permission.

For the purpose of this policy, confidentiality relates to the transmission of personal, sensitive or identifiable information about individuals or organisation's (confidential information), which comes into the possession of an Organisation through its work.

The Forum holds personal data about its staff, directors, sub-contractors, users, members, customers and visitors as well as financial information in relation to the Forum's business, which may include that of others/other organisation's whom work with us, which will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside of the organisation without prior permission.

All personal data will be dealt with sensitively and in the strictest confidence internally and externally.

Confidentiality, as a stand-alone policy element is a reinforcement of other elements in this policy including GDPR and is reiterated to ensure that all persons as mentioned above, but not limited to,

understand the Forum's requirements in relation to the disclosure of personal data and confidential information in addition to the consequences of any breach in confidentiality.

Principles

- All personal paper-based and electronic data must be stored in accordance with the GDPR Act 2018 and must be secured against unauthorised access, accidental disclosure, loss or destruction.
- All personal paper-based and electronic data must only be accessible to those individuals authorised to have access.
- All statistical records given to third parties, such as to support funding applications or monitoring reports shall be produced wherever possible in anonymous form, so individuals cannot be recognised.

Records

All records are kept in locked filing cabinets. All information relating to employees or clients will be left in locked drawers. This includes notebooks, copies of correspondence and any other sources of information.

Acceptable Breaches of Confidentiality

The Forum recognises that occasions may arise where individual workers feel they need to breach confidentiality. Confidential or sensitive information relating to an individual may be divulged where there is risk of danger to the individual, a volunteer or employee, or the public at large, or where it is against the law to withhold it. In these circumstances, information may be divulged to external agencies e.g. police or social services on a need to know basis. Where a worker feels confidentiality should be breached the following steps will be taken:

- The worker should raise the matter immediately with the General Manager.
- The worker must discuss with the General Manager the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved by breaching confidentiality. The General Manager should take a written note of this discussion.
- The General Manager is responsible for discussing with the worker what options are available in each set of circumstances.
- The General Manager is responsible for making a decision on whether confidentiality should be breached. If the General Manager decides that confidentiality is to be breached then they should take the following steps:

  The General Manager should record all details and depending on the nature of the circumstance, contact or keep the Chair informed. Where the Chair/Vice Chair has been informed, information given to the Chair should be brief so as not to overly/further disclose information on the full facts of the case, ensuring they do not breach confidentiality in doing so. The General Manager should seek authorisation to breach confidentiality from the Chair/Vice Chair where consequences could be damaging to the organisation. If the Chair/Vice Chair agrees to breach confidentiality, a full written report on the case should be made and any action agreed undertaken. The Line Manager is responsible for ensuring all activities are actioned. If the Chair/Vice Chair does not agree to

breach confidentiality then this is the final decision of the Forum and again a report should be compiled.

Legislative Framework

The Forum will monitor this policy to ensure it meets statutory and legal requirements including any other related legislation i.e. GDPR, Children's Act, Rehabilitation of Offenders Act and Prevention of Terrorism Act as an example.

Common Law

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges. Common Law is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent. The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. In practice, this means that all employee/client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the employee/client.

It is irrelevant for example how old the employee/client is, or what the state of his/her mental health is; the duty still applies.

Three circumstances making disclosure of confidential information lawful are:

· where the individual to whom the information relates has consented
· where disclosure is necessary to safeguard the individual, or others, or is in the public interest
· where there is a legal duty to do so, for example a court order

Therefore, under the common law, an organisation wishing to disclose an employee's/client's personal information to anyone outside the project/HR should first seek the consent of that employee/client.

Where this is not possible, an organisation may be able to rely on disclosure being in the overriding safeguarding interest of the individual or others or in the public interest. However, whether a disclosure is in the public interest is not a decision to be taken lightly. Solid justification is required before individual rights are set aside and specialist or legal advice should be sought before the information is disclosed. Any decision to disclose should be fully documented. Disclosures required by court order should be referred to the organisation's legal advisors as promptly as possible, so that any necessary representations may be made to the court, for example to limit the information requested. If a disclosure is made which is not permitted under common law the employee/client could possibly bring a legal action not only against the organisation but also against the individual responsible for the breach.

Records management considerations

All persons involved in the records management function should be aware of their responsibility for maintaining confidentiality of records.

- Employees should only have access to those parts of the record required to carry out their role.
- Requests for records access by other staff members should be logged or authority requested by the General Manager.
- Particular care should be taken during the transportation of any employee/client records outside of the organisational site, for example security envelopes and approved carriers should be used where necessary.

D. <u>General Data Protection Regulations Policy (2018)</u>

The General Data Protection Regulation (GDPR) Policy 2018 supersedes the Data Protection Act 1998 (directive 95/46/EC) with effect from 25th May 2018, affecting all UK companies who process or store personal information.

The GDPR policy is focused on looking after the privacy and rights of the individual, and based on the premise that consumers and data subjects should have knowledge of what data is held about them, how it's held, and other core information that the Data Protection Act did not originally demand. Whilst it's designed to strengthen and unify data protection for individuals within the European Union, it also deals with the export of personal data outside the EU too. A Privacy Policy is internally focused, telling employees what they may do with personal information, while a privacy notice is externally facing, telling customers, regulators and other stakeholders what the organisation does with personal information.

AIMS OF THIS POLICY

The Food and Drink Forum needs to keep certain information on its employees, consultants and service users to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with, in line with said General Data Protection Regulations. In order to comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation. This policy covers employed staff, contractors and Directors.

PRINCIPLES

The eight Data Protection Act 1998 principles have been superseded by the six, more modern and more in depth General Data Protection Regulation (GDPR) principles. Also, the Data Protection Act 1998 will be outdated by the forthcoming Data Protection Bill (which will incorporate the GDPR content), we should no longer consider the eight Data Protection Principles but instead, consider the six GDPR Principles.

These principles are:

- Lawfulness, fairness and transparency
- Purpose limitations
- Data minimisation
- Accuracy
- Storage limitations
- Integrity and confidentiality

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.:

- **Accountability:** Those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

TYPES OF INFORMATION PROCESSED

The Food and Drink Forum processes the following personal information:

- Personal details
- Family details
- Business activities of the person whose personal information we are processing
- Financial details
- Training details
- Education and employment details
- Goods and services
- Physical or mental health details
- Racial or ethnic origin
- Religious or other beliefs

Personal information is kept in the following forms:

- Paper based systems
- Computer based systems

Groups of people within the organisation who will process personal information are:

- Customers
- Clients
- Funding Bodies
- Directors
- Trainers
- Employees
- Suppliers
- Professional advisers and consultants
- Complainants, enquirers

NOTIFICATION

The needs of The Food and Drink Forum for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires. If there are any interim changes, these will be notified to the Information Commissioner within 28 days. The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is The Food and Drink Forum.

RESPONSIBILITIES

Under the Data Protection Guardianship Code, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of The Food and Drink Forum this is the Board of Non-Executive Directors. The governing body delegates tasks to the Data Controller. The Data Controller is responsible for:

- Understanding and communicating obligations under the Act
- Identifying potential problem areas or risks
- Producing clear and effective procedures
- Notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes

All those who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles. Breach of this policy will result in disciplinary proceedings for employed staff or termination of the consultant's agreement, or dismissal of a director from the board.

POLICY IMPLEMENTATION

To meet our responsibilities staff will:

- Ensure any personal data is collected in a fair and lawful way
- Explain why it is needed at the start
- Ensure that only the minimum amount of information needed is collected and used
- Ensure the information used is up to date and accurate
- Review the length of time information is held
- Ensure it is kept safely
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do
- Any disclosure of personal data will be in line with our procedures
- Queries about handling personal information will be dealt with swiftly and politely

TRAINING

Training and awareness raising about the Data Protection Act and how it is followed in this organisation will take the following forms:

- **On induction**: The data protection policy is provided to all new staff and briefing is given on handling and secure storage of personal information.
- **General training/awareness raising**: On the job training includes awareness of receiving and handling of personal data in line with this policy and the data protection principles.

GATHERING AND CHECKING INFORMATION

Before personal information is collected, we will consider:

- What details are necessary for your purposes
- How long you are likely to need this information
- Why the information is being gathered
- What the information will be used for
- Who will have access to their information (including third parties)

We will inform people whose information is gathered about the following:

- Why the information is being gathered
- What the information will be used for
- Who will have access to their information (including third parties)

We will take the following measures to ensure that personal information kept is accurate:

- The terms and conditions of our Employee Handbook state that employees are required to inform us of any changes to personal information
- An annual reminder to update all personal information if necessary is given at appraisal meetings

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

DATA SECURITY

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Using internal lockable cupboards and or external large storage containers with restricted access to keys
- Password protection on all personal information files
- Computer systems will be set up with restricted access to certain areas
- No personal data will usually be taken off site either as hard copy, on laptop or on memory stick
- If personal data must be taken off site, either on paper, memory stick or laptop it must not be left unattended and care must be taken to prevent access by unauthorised persons. Memory sticks must be Federal Information Processing Standards (FIPS) compliant
- Data on computers is backed up to the cloud
- Password protection is used for attachments containing sensitive personal information sent by email. Passwords must be sent separately or by other means
- Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings.
- The Board are accountable for compliance of this policy. A director could be personally liable for any penalty arising from a breach that they have made.
- Any unauthorised disclosure made by a consultant may result in the termination of the agreement.
- Information will only be shared with other agencies under the following circumstances:
    - to ensure the safety and welfare of the service user
    - where such information is relevant to the employment arrangements and specific requirements of the employee or client

- where such information is required to ensure the safety and welfare of the persons concerned
- to protect the safety and welfare of a child or other adult who may be at risk within the Company
- where clients/services users have agreed to funded or other support and data reports are required as part of the funding/contractual requirements

SUBJECT ACCESS REQUESTS (SAR)

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to the General Manager. "In writing" can be by paper, fax, e-mail and even using the organisation's social media pages, although the results of a SAR must never be issued to the recipient using social media. The following information will be required before access is granted:

- Full name and contact details of the person making the request, including a telephone number
- Their relationship with the organisation (former/current member of staff, trustee or other volunteer, service user)
- Any information used by the organisation to differentiate them from others with the same name (account number, unique ID, student number, etc.,)
- Details of specific information they require and any relevant dates (e.g. courses attended between two dates, tutor notes, e-mails from 2013-present, etc.).
- Those submitting a SAR may ask about the logic involved in any automated processes made about them

Queries about handling personal information will be dealt with swiftly and politely. We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 Calendar days required by the Act. These 40 days do not begin until we have received all vital information required to deliver the results, as well as cleared Administrative charge payment. Payments are not considered made until funds are cleared in our account.

Link for help on SARs at the ICO's website: https://ico.org.uk/for-the-public/personal-information/ Checklist for SARs (ICO Website). https://ico.org.uk/for-organisations/subject-access-request-checklist/

The IT & Data Confidentiality, Storage, Security & GDPR Policy is followed by an Employee/Contractor/Director declaration form which must be read and signed by all.

E. POLICY DECLARATION

THE FOOD AND DRINK FORUM LIMITED

IT & Data Confidentiality, Storage, Security & General Data Protection Regulation Policy Declaration Form

DECLARATION

I confirm I have read and understood The Food and Drink Forum's **IT & Data Confidentiality, Storage, Security & General Data Protection Regulation Policy** and will act in accordance with my role and responsibilities and the Policy guidance, rules and procedures and any legislative updates. I am also fully aware of the consequences of any breach of the Policy.

I am connected with this organisation in my capacity as:

- ☐ An Employee
- ☐ A Consultant / Contractor
- ☐ A Director

Signature:

Print name:

Date:

Please return this form to Bryony Whiley (bryony.whiley@foodanddrinkforum.co.uk or send to The Food & Drink Forum, The Business Centre, Southglade Food Park, Gala Way, Nottingham, NG5 9RG).