


TEAM FUSION	
DATA PROTECTION POLICY INCORPORATING GDPR	
COMPANY POLICIES	

1. Introduction

Team Fusion is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. It is also necessary to process information so that Team Fusion can comply with its legal obligations. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

Team Fusion must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 and specifically to the UK General Data Protection Regulation (GDPR) May 2018. Following the UK leaving the European Union on 31 December 2020, the UK GDPR replaced the EU GDPR May 2018. All the main principles, obligations and rights remain in place.

Team Fusion is registered with the Information Commissioner's Office and a copy of the Register Entry Report is saved in SharePoint.

The May 2018 GDPR regulatory environment demands higher transparency and accountability in how companies manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.


The GDPR contains provisions that Team Fusion will need to be aware of as data controllers, including provisions intended to enhance the protection of customer's and employees' personal data. For example, the GDPR requires that we must ensure that our privacy notices are written in a clear, plain way that staff and customers will understand.

Team Fusion needs to process certain information about its staff, customers and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- The administration of 3rd party emergency planning and risk assessments
- The administration of training programmes and courses
- Recording staff training, attendance and conduct
- Complying with legal obligations to funding bodies and government including local government
- The development of standard operating procedures and casualty retrieval plans
- Examinations and external accreditation
- The recruitment and payment of staff
- Publication of Team Fusion' Board of Directors and employee's names and contact information

UNCONTROLLED COPY IF PRINTED

No. of Pages = 12

TEAM FUSION	
DATA PROTECTION POLICY INCORPORATING GDPR	
COMPANY POLICIES	

2. Compliance

To comply with various legal obligations, including the obligations imposed on it by the Data Protection Act 2018 and General Data Protection Regulation 2018, Team Fusion must ensure that all information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully. To ensure this, Team Fusion has developed this Data Protection Policy and the accompanying Data Protection Code of Practice. This policy applies to all staff and customers.

Any breach of this policy or of the Regulation itself will be considered an offence and the company's disciplinary procedures will be invoked. As a matter of best practice, other agencies and individuals working with Team Fusion and who have access to personal information, will be expected to read and comply with this policy. Data Processors will be expected to sign a data agreement and it is the responsibility of those initiating the relationship to notify the Team Fusion Data Protection Representative to ensure the agreement is put in place.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

3. UK General Data Protection Regulation May 2018 (GDPR)

GDPR came into force on the 25th May 2018. It regulates the processing of personal data and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data that relates to them. On 31 December 2020 after UK left the European Union, UK GDPR replaced EU GDPR. All the main principles, obligations and rights remain in place.

Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.


4. Responsibilities

Team Fusion as a body corporate is the Data Controller under the terms of the 2018 Act and GDPR legislation.

Team Fusion will be the 'data controller'— this means it is ultimately responsible for controlling the use and processing of the personal data.

Team Fusion has appointed a Data Protection Representative, who is responsible for addressing any initial concerns regarding the personal data held by Team Fusion and how it is processed, held and used.

The Senior Leadership Team (Managing Director and Chief Operating Officer) is responsible for all day-to-day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the company.

TEAM FUSION	
DATA PROTECTION POLICY INCORPORATING GDPR	
COMPANY POLICIES	

The Senior Leadership Team is also responsible for ensuring that the company's notification is kept accurate. Details of the company's notification can be found on the Office of the Information Commissioner's website.

Our data registration number is: Z1201074

Compliance with the legislation is the personal responsibility of all members of the company who process personal information.

Individuals who provide personal data to the company are responsible for ensuring that the information is accurate and up-to-date.

5. Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles.

In order to comply with its obligations, Team Fusion undertakes to adhere to the eight principles.

5.1 Process personal data fairly and lawfully

Team Fusion will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged, an indication of the period for which the data will be kept and any other information that may be relevant.

5.2 Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose

Team Fusion will ensure that the reason it collected the data originally is the only reason it processes that data, unless the individual is informed of any additional processing before it takes place.


5.3 Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed

Team Fusion will not seek to collect any personal data that is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data is given by individuals, it will be destroyed immediately.

5.4 Keep personal data accurate and, where necessary, up to date

Team Fusion will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and individuals should notify the company if, for example, a change in circumstances means that the data needs to be updated. It is the responsibility of the company to ensure that any notification regarding the change is noted and acted on.

5.5 Only keep personal data for as long as is necessary

TEAM FUSION	
DATA PROTECTION POLICY INCORPORATING GDPR	
COMPANY POLICIES	

Team Fusion undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation and any other statutory requirements. This means Team Fusion will undertake a regular review of the information held and implement a clearing process.

Team Fusion will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

5.6 Process personal data in accordance with the rights of the data subject under the legislation

GDPR put into practice eight rights for individuals which are:

- The right to be informed
- The right to access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision- making including profiling

Team Fusion will only process personal data in accordance with individuals' rights.

5.7 Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data


All members of staff are responsible for ensuring that any personal data they hold is kept securely and not disclosed to any unauthorised third parties.

Team Fusion will ensure that all personal data is accessible only to those who have a valid reason for using it.

Team Fusion will have in place appropriate security measures for:

- keeping all personal data in a lockable cabinet with key-controlled access
- password protecting personal data held electronically
- archiving personal data which are then kept securely (lockable cabinet)
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff
- ensuring that PC screens are not left unattended without a password protected screen-saver being used

In addition, Team Fusion will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work.

TEAM FUSION	
DATA PROTECTION POLICY INCORPORATING GDPR	
COMPANY POLICIES	

Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff who process personal data 'off-site', e.g. when working at home and, in those circumstances, additional care must be taken regarding the security of the data.

- 5.8 Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Team Fusion will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the Internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA – so Team Fusion will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If the company collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

6. Consent as a Basis for Processing

Although it is not always necessary to gain consent from individuals before processing their data, it is sometimes the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when Team Fusion is processing any sensitive data, as defined by the legislation.

Team Fusion understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. permission via email) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained based on misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.


Team Fusion will ensure that any forms used to gather data on an individual will contain the following fair collection statement explaining the use of that data, how the data may be disclosed and indicate if the individual needs to consent to the processing.

“for the purposes of the General Data Protection Regulation (GDPR) you consent to the company holding and processing personal data including sensitive personal data of which you are the subject, details of which are specified in the company’s data protection policy. This will include marketing images and the company CCTV.”

The user must be given the opportunity to opt select Yes or No.

7. Subject access Rights (SARs)

Individuals have a right to access any personal data relating to them that is held by the company. Any individual wishing to exercise this right should apply in writing to the Data

TEAM FUSION	
DATA PROTECTION POLICY INCORPORATING GDPR	
COMPANY POLICIES	

Protection Representative (DPR). Any member of staff receiving a SAR should forward this to the DPA.

Under the terms of the legislation, any such requests must be complied with within 30 days.

8. Disclosure of Data

Only disclosures that have been notified under the company's DP notification must be made and staff should exercise caution when asked to disclose personal data held about another individual or third party.

Team Fusion undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

the individual has given their consent to the disclosure
the disclosure is in the legitimate interests of the company
the disclosure is required for the performance of a contract

There are other instances when the legislation permits disclosure without the consent of the individual. Please follow this link to the ICO's website (www.ico.org.uk), which provides further detailed guidance.

In no circumstances will Team Fusion sell any of its databases to a third party.

9. Publication of Company Information

Team Fusion publishes various items that may include some personal data, e.g.

- internal telephone directory
- event information
- photos and information in marketing materials i.e. Company website


It may be that, in some circumstances, an individual wishes their data processed for such reasons to be kept confidential, or restricted company access only. Therefore, it is Team Fusion policy to offer an opportunity to opt-out of the publication of such when collecting the information.

10. Email

It is the policy of Team Fusion to ensure that senders and recipients of email are made aware that, under the DPA and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the sender's email.

11. Procedure for Review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 2018.

TEAM FUSION	
DATA PROTECTION POLICY INCORPORATING GDPR	
COMPANY POLICIES	

Please follow this link to the ICO's website (www.ico.org.uk), which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc.


In particular, you may find it helpful to read the Guide to Data Protection, which is available from the website.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact the appropriate Designated Data Controller, who would be:

- For employees: Chief Operating Officer
- For customers and all others: Chief Operating Officer

12. Data Protection Code of Practice

1. **Introduction** - This Code of Practice must be read in conjunction with the Team Fusion Data Protection Policy document and the Information Commissioner's Officer Register Entry Report to give the fullest picture of Team Fusion's data protection regime. This document gives an introduction to some basic points of practice relating to the handling and processing of personal data at Team Fusion. It also lists the particular activities carried out within the Team Fusion administrative and training departments that involve the handling and processing of personal data.
2. **Key Concepts** - The Data Protection Act 2018 and UK General Data Protection Regulation (GDPR) May 2018 places an obligation upon Team Fusion, as a data controller, to collect and use personal data in a responsible and accountable fashion. Team Fusion is committed to ensuring that every current employee, customer and client complies with these Acts to ensure the confidentiality of any personal data held by the Team Fusion in whatever medium. Three key concepts to be considered are those of purpose, fairness and transparency.
3. **Purpose** - Data controllers can only process personal data where they have a clear purpose for doing so and then only as necessitated by that purpose. Personal data cannot be processed for purposes that have not been defined and declared in the Team Fusion Data Protection Register entry (see paragraph 6 below).
4. **Fairness** - In defining the purposes for which Team Fusion processes personal data, the fairness of that processing must be considered. For some types of processing the required elements of fairness and legality are clearly outlined in the legislation, but for many others they are not. In such cases, Team Fusion has tried to take a broad approach to deciding what is fair in each case, based on an interpretation of the 1998 and 2018 Acts and in conjunction with advice from the Information Commissioner, the Team Fusion's own legal advisors.
5. **Transparency** - Members of staff others must be able to feel that there is no intention to hide from them details of how their personal data are collected,

TEAM FUSION	
DATA PROTECTION POLICY INCORPORATING GDPR	
COMPANY POLICIES	

used and distributed by Team Fusion. One of the functions of this Code of Practice is to provide that assurance.

6. **Existing Notifications** - The Act requires many data controllers to notify the Information Commissioner of the purposes for which personal data are processed, together with certain details of that processing. Those notifications are then held on a public register.
7. It is an offence for Team Fusion to hold personal data that falls outside of the classes declared in these notifications or to process personal data for any purposes that are not defined there. It is therefore very important that those who work with personal data in the course of their employment or learning are familiar with the details contained in these notifications.
8. Any changes that may be required should be passed to the Team Fusion administration personnel as these entries are periodically reviewed and amended as necessary by the Board of Directors.
9. Paragraph 33 of this Code of Practice gives details of Team Fusion Designated Data Controllers, who are responsible for handling subject access requests and dealing with data protection enquiries within the company.

Collection and Amendment of Personal Data

10. **Collection of personal data** - In most cases, the personal data held by Team Fusion will be obtained directly from the data subjects themselves. The law stipulates that a data protection notice must accompany any request for personal data. Any employees responsible for managing the collection of personal data for the legitimate activities of the company must ensure that a notice containing the following information is included in the request for that data:
 - A statement that Team Fusion is the data controller
 - The name and or job title of the specific employee responsible for the administration of the personal data being collected, to enable, for example, subsequent amendments to be submitted by the data subject
 - A clear explanation of the types of data being collected and the purposes for which that data will be processed
 - Any further information that is considered necessary to ensure that the data processing can be described as being fair, for example details of any third parties to whom the data might be disclosed
 - A statement making it clear that by submitting the personal data, the data subjects are giving their consent for the processing of the data for the stated purposes to take place.
11. **Amendment of personal data** - From time to time data subjects will wish to update some of their personal data held by Team Fusion, for example their home addresses or other contact details previously submitted. To do this, the

data subjects must either contact the specific member of staff designated in the data protection notice at the time the data was submitted, or the appropriate Designated Data Controller as set out in paragraph 33. Proof of identity will be required before any amendments can be made.

12. As and when 'self-service' computer-based administrative systems are introduced for employees, customers, students or others, the data subjects themselves will be able to take responsibility for the maintenance of certain elements of their personal records.
13. These systems will incorporate the necessary authentication and security mechanisms to ensure that data subjects are only able to view and amend their own data.
14. **Security of personal data** - Of fundamental importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside Team Fusion. Authorised disclosures or transfers are those that are defined within the appropriate Notifications and declared to the data subject either at the point of data collection or subsequently, the necessary consent for disclosure or transfer having been obtained if required.
15. To help ensure the security of personal data within Team Fusion, all those employees who process such data in the course of performing their duties are required to follow the general guidelines set out below.
16. **Secure storage of personal data** - Each employee whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage, in line with the Team Fusion Data Protection Policy, which states that personal data should:
 - Be kept in a locked filing cabinet, drawer, or safe
 - or*
 - If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up
 - and*
 - If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.
17. Ordinarily, personal data should never be stored except for operational reasons at employees' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.
18. Employees should be aware that log files would record details of all users who access, alter or delete or attempt to access, alter or delete centrally held computerised databases and files containing personal data.
19. **Secure processing of personal data** - While staff members in the course of performing their legitimate duties are using personal data, reasonable

precautions must be taken to ensure the safety and privacy of that data. For example:

- In open-plan offices, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised persons may readily see that data, and password protected screensavers should be used.
 - Personal data in manual form, such as in paper files, correspondence or database printouts, should not be left in view in open-plan offices while the relevant employees are away from their desks. They should instead be locked away or at least covered.
 - Where manual records containing personal data are accessible to a number of employees in the course of their legitimate activities, access logbooks should be used where practicable to help monitor the whereabouts and use of such records.
20. Ordinarily, personal data should not be processed at employees' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Data Controller must be obtained, and all the security guidelines given in this document must still be followed.

The disclosure and transfer of personal data


21. **Authorised and unauthorised disclosures** - Employees working with personal data will be made aware by their line managers or other appropriate staff of the purposes for which the data is processed and the legitimate parties either within or outside Team Fusion to whom that data, either in whole or in part, may be disclosed or transferred. Personal information must not be disclosed either orally or in writing or via Web pages or by any other means, manual or electronic, accidentally or otherwise, to any unauthorised third party.
22. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.
23. **Security of data during transfer** - Where personal data is transferred between employees of Team Fusion during their legitimate activities, the level of security appropriate to the type of data and anticipated risks should be applied. For example, sensitive personal data should either be transferred by internal mail in sealed envelopes or by hand. If transferred by e-mail, such data should normally either be encrypted or sent in a password-protected attachment (for example using Microsoft Word's 'require password to open' feature), with the password being supplied separately.
24. **Disclosures outside Team Fusion** - When a request to disclose or amend personal data relating to an employee, customer or client is received from an individual or organization outside the company, in general no data should be disclosed or amended unless the authority and authenticity of the request can be established. Disclosures requested by those claiming to be relatives or

friends should be refused unless the consent of the data subject is obtained for such disclosures or in one of the few situations where disclosure without consent is permitted by the law.

25. Requests for the disclosure of personal data from the Police, Government bodies, the British Council or other official bodies and agencies should be investigated sufficiently to verify the authenticity of the request and may then be acted upon if there is a legal requirement for such disclosure or the consent of the data subject has been given for the disclosure.

Publication of Team Fusion Information

26. While the majority of personal data held by Team Fusion is processed for internal administrative purposes and is never disclosed outside the company, some categories of data are routinely or from time to time released through one or more forms of publication.
27. **Staff Directory** - In order to meet the legitimate needs of customers, visitors and enquirers to be able to make contact with appropriate staff, Team Fusion may make available on its public web site a directory containing the job title, title, forename, surname and office e-mail address of each staff member. However, at the time of appointment and at any time while in post (via a request to the designated Data Controller) each individual member of staff will be able to specify the level of detail that will appear in this public directory, i.e. being able to request that the following be omitted: title, forename, e-mail address. A printed directory is made available to all members of staff within the company, but is not ordinarily given to anyone else.
28. **Staff personal data on web pages** - Apart from the staff directory described above, staff biographical details or other personal data may be published on the Team Fusion web site (www.teamfusion.com) or in other media, but only where the staff concerned have given their consent for such information to be made publicly available. However, publication in this way does not mean that such data have been placed into the public domain. Team Fusion retains control and copyright of such data, and the data must not be reproduced or further processed without the company's express permission.
29. **The retention of personal data** - Team Fusion has a duty to retain some employee and personal data for a period of time following their departure from the company, mainly for legal reasons, but also for other purposes such as being able to provide personal and academic references, or for financial reasons, for example relating to pensions and taxation. Different categories of data will be retained for different periods of time.
30. **The disposal of personal data** - When a record containing personal data is to be disposed of, the following procedures will be followed:
 - All paper or microfilm documentation containing personal data will be permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data

TEAM FUSION	
DATA PROTECTION POLICY INCORPORATING GDPR	
COMPANY POLICIES	

- All computer equipment or media that are to be sold or scrapped will have had all personal data destroyed, by re-formatting, over-writing or degaussing.
 - Details of the destruction of data will be logged in both instances mentioned above.
31. Employees will be provided with guidance as to the correct mechanisms for disposal of different types of personal data and audits will be carried out to ensure that this guidance is adhered to. Employees will be made aware that erasing/deleting electronic files does not equate to destroying them.

Subject Access Requests

32. Individuals have a right to access any personal data relating to them that is held by the company. Any individual wishing to exercise this right should apply in writing to the Data Protection Processor (DPP). Any member of staff receiving a SAR should forward this to the DPA.
33. Under the terms of the legislation, any such requests must be complied with within 30 days.

Compliance with these policies is mandatory for all Company personnel.



Jerry Jones
Managing Director

March 2021

First Issued: March 2021