Data Protection Policy

Policy information	
Organisation	**Information For Patients Leaflets**
Scope of policy	Policy applies to our only office in Henley on Thames.
Policy operational date	20th May 2018
Policy prepared by	David Hammond
Date approved by Board/ Management Committee	20th May 2018
Policy review date	19th May 2021

Introduction	
Purpose of policy	Reason for the Policy: • complying with the GDPR Law • Following good practice • Protecting clients, staff and other individuals. • Protecting the organisation from data breaches.
Types of data	Data IFP Holds • Company contact details. • Existing Clients data and contact details.

Policy statement	At IFP we are committed to: • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently • Notify the Information Commissioner voluntarily, even if this is not required Please note the guidance from ICO on when breaches should be reported as this is one of the main changes from the current Data Protection Act and GDPR (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/)
Key risks	IFP Risks are: • Information about data getting into the wrong hands. • Individuals being harmed through data being inaccurate or insufficient.

Responsibilities	
Company Director	They have overall responsibility for ensuring that the organisation complies with its legal obligations. Managing Director of IFP is David Hammond
Data Protection Officer	Their responsibilities include: • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Specific Department Heads	N/A
Employees	All staff members are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.
Enforcement	There will be strong penalties for any infringement of the Data Protection policies, and we have training in place so staff members are aware of the consequences. Any data protection issues will be dealt with quickly and efficiently.

Security	
Scope	Data Security is not wholly a Data Protection issue. Business Continuity is included below.
Setting security levels	The greater the consequences of a breach of confidentiality, the tighter the security will be.
Security measures	We have many security measures in place: • Password Protection on all computers, and all accounting software, and on our backup. • Entry control, if there is no one in the office, the door is locked and we have an alarm • There is a tidy desk policy in the reception room, no papers left out and no 'easy to grab' sheets. • All important data is not kept in the main room, and any unneeded data will be destroyed.
Business continuity	The data on the computers is backed up through a software in the cloud. This is password protected and is cleared regularly of unwanted data. All the computers have the same security procedures for the different software.
Specific risks	If information is in particular risk of being exposed - in meetings or with clients, then added precautions are taken. Such as clearing desks, taking data back to the office, being specific in what data is needed for the meeting before using it. "vishing" or "phishing" are an important aspect to make sure the staff are aware of, and this is in the training they learn that these risks - where employees are tricked into giving away information over the phone or by email – are warned of and how to avoid. Common situations which are key issues include whether contact details may be given over the phone and to make sure this doesn't happen without their consent.
Data recording and storage	
Accuracy	The measures which are key to making sure the data that is kept is accurate. Including double checking data with the clients every few months to make sure their contact details haven't changed. Also ask if they need to change any more personal details or banking details, to make sure they are all up to date.
Updating	The data held is checked every few months with regular clients, and every year the data is checked with older clients.

Storage	Accounting and banking data is held away from where the public can access it, and all personal data is also held away from where the public would be able to access it.
Archiving	The procedure for archiving or destroying data is the data is held until the client asked for it to be removed, or after 3 years the data will be destroyed if not needed. The paper data will be shredded either in house or outsourced depending on quantity, and digital data will be deleted from the system and the back up.
Right of Access	
Responsibility	David Hammond is in charge of ensuring that right of access requests are handled within the legal time limit which is one month.
Procedure for making request	Right of access requests must be in writing. We will supply a standard form to fill out if needed. If any employees receive any right of access requests, they must inform either David and they will deal with it as soon as possible.
Provision for verifying identity	Any identity issues for data requests will be verified by the people responsible, either by personal meeting or phone verification with a member of staff who has dealt with the client before.
Charging	The information will be provided free of charge. However the charge of a 'reasonable fee' will apply when a request is manifestly unfounded or excessive, particularly if it is repetitive. IFP may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that IFP can charge for all subsequent access requests. The fee will be based on the administrative cost of providing the information.
Procedure for granting access	If the request is made electronically, IFP will provide the information in a commonly used electronic format. For example, by email.
Transparency	

Commitment	IFP is transparent when it comes to the commitment to ensure that the Data it holds is secure. • Data is processed for work the client has requested/ invoicing/assistance in conferences/office services.
Procedure	Each type of Data Subject is to be informed by the use of: • the handbook for employees • in the welcome form for new clients • during the initial interview with clients • on the web site
Responsibility	All the responsibility for the data policy transparency falls on the managing director.

Lawful Basis

Underlying principles	GDPR states you must record the lawful basis for the personal data you hold and you should set your basis for each Data Subject type here (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/)
Opting out	IFP rarely send out any marketing of any kind, but when this does occur there will be a clear way in the email to opt out of future marketing content.
Withdrawing consent	IFP Acknowledges that once given, consent can be withdrawn, but not retrospectively. There may be occasions where IFP has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn. When this does occur, no marketing will be sent out or used irresponsibly.

Employee training & Acceptance of responsibilities

Induction	All employees who have access to any kind of personal data are aware of their responsibilities, these have been outlined during the induction procedures.
Continuing training	If any employees need more training or a top up to the Data Protection policy, this will be given.
Procedure for staff signifying acceptance of policy	Policy will be included in the Company handbook, and a signed form by all employees to acknowledge they have read and understood the policy.

Policy review	
Responsibility	Mark Hawkins – Managing Director will carry out all reviews of the policy.
Procedure	David Hammond will also be consulted with the procedure.
Timing	A review of the current data policy will take approximately 3 days, this will be accounted for and complete before the date.

For any queries on this policy please call 01491 577307
Or email linda.woodward@ifpleaflets.co.uk