Policy information - Data Protection Policy – Template	
Organisation	This should be the Data Controller (see notes). If you are a sold trader or independent practitioner – that's you. If you see clients under a business name, list the business.
Scope of policy	If you are a sole practitioner you would write here that the policy applies to you and your clients. If you hire staff, and have multiple locations that you work in, you would need to add where the responsibility for data is in each location and what the policy applies to. For example, if you work for a clinic, it may be that customer data is covered by the clinic's policy. If you see clients at home, your policy will cover the data you process and hold at home.
Policy operational date	Should start now, but you can add a slightly later date here if you are not quite ready yet.
Policy prepared by	Here you should state your name if you are a sole trader, or the company name if you operate under a company.
Date approved by Board/ Management Committee	This section is only relevant if you have a board or management committee. If you are a sole trader, or sole practitioner – this part is not relevant for you.
Policy review date	It is probably sufficient to review a Data Protection policy every three years.
Introduction	
Purpose of policy	This could include: • complying with the law • following good practice • protecting clients, staff and other individuals • protecting the organisation (if you are larger than one person)
Brief introduction to Data Protection Act 1998	It is not essential to include a summary of the Act, but you may find it helpful.
Data Protection Principles	Again, it is not essential to include the Principles, but it may be useful
Personal data	Although good practice will often apply to information which is technically outside the scope of the Data Protection Act, it may be useful to set out which information is covered, and — equally importantly — which is not. For practitioners this is likely to be: • Case taking files • Clinical test results • Email addresses • Prescription files • Images of eyes (for iridologists)
Policy statement	This could include a commitment 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 (see notes) the Information Commissioner voluntarily, even if this is not required.

Key risks	This could identify the main risks within your organisation in two key areas: • information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information • individuals being harmed through data being inaccurate or insufficient
Responsibilities	
Data Protection Officer	There is no "right" person for this to be. It should be the most senior person. Their responsibilities include: • Briefing new staff on data protection • Reviewing Data Protection and related policies • Ensuring that Data Protection induction and training takes place whenever someone is hired • Notification (see notes) • Handling subject access requests from clients wanting to access or delete their data • Approving unusual or controversial disclosures of personal data Approving contracts with Data Processors such as external payment processors like PayPal, or mailing software like MailChimp (see notes)
Specific other staff	• If you have other staff such as dispensary assistant, or receptionist or other role – and that person has access to data (such as name address, or anything which may identify a person) – you will have to include in your policy that staff will have access to data for the purpose of their job.
Team/Department managers	If you have a large health centre, or multiple centres – each department will need to create a policy related to their department. For example, if you work in a clinic and rent out spaces – each occupier of the space will need a policy for their own area. That area will need to go through the same steps of data protection that you are. Also, the managers must ensure that the Data Protection Officer is informed of any changes in their uses of personal data that might affect the organisation's Notification.
Staff & volunteers	All staff and volunteers should be 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. (From now on, where 'staff' is used, this includes both paid staff and volunteers.)
Enforcement	You may want to say what the penalties are for infringing the Data Protection and related policies. These penalties are usually disciplinary ones. Extreme data breaches can be reported to ICO directly.
Confidentiality	

Scope	Confidentiality applies to a much wider range of information than Data Protection. It may be better to have a completely separate Confidentiality Policy. If confidentiality is included in the Data Protection policy, it must be made clear that they do not cover the same things. Some of the things that are likely to be confidential, but may well not be subject to Data Protection, include: • Information about your clients • Information about their children or extended family • Information which is not recorded, either on paper or electronically, such as their emotional condition or aspects of their lives which are private and only revealed to you • Information that may be private and / or embarrassing to them Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act
Understanding of confidentiality	It is important to set out who has access, to which data, for which purposes. Access in this case means not just by staff, but also by people outside the organisation. Normally access will be defined on a "need to know" basis; no one should have access to information unless it is relevant to their work. This may be relaxed in the case of information which poses a low risk: for example a list of business contacts may be made generally available, even if this means people having access who don't strictly need it. Where risks can be specifically identified, it may be worth making provision in the policy: for example in work with teenagers, discussing how much information will be shared with their parents. • The limits to confidentiality must also be set out. There will always be cases where the organisation feels it is right to break confidentiality, and there should be a procedure for deciding on a case-by-case basis whether this is appropriate.
Communication with Data Subjects	It is worth describing how clients, staff and other Data Subjects will be informed about confidentiality, so that there is minimal risk of them being surprised at any later stage to find out that who has information about them.
Communication with staff	It is worth describing how staff will be informed and trained in their responsibilities, and also what the procedure is if they have any questions about whether information should be disclosed, or access allowed.
Authorisation for disclosures not directly related to the reason why data is held	These fall into two main categories: those likely to be at the instigation, or in the interests, of the Data Subject, and those which are made in the course of official investigations. For the first (such as a financial reference request from a bank), consent from the Data Subject is likely to be the normal authorisation. This consent should be recorded. For the second, it may be appropriate for the Data Subject not even to be informed; authorisation should be made at a senior level within your organisation.
Security	

Scope	Security must not be confused with confidentiality. The latter is about defining what is allowed — setting the boundary; the former is about ensuring that the boundary is maintained. However, there must be a relationship between the two. Like confidentiality, security is not wholly a Data Protection issue. Again, a separate policy may be preferable. The entries for business continuity and personal security below are those with least Data Protection relevance.
Setting security levels	The greater the consequences of a breach of confidentiality, the tighter the security should be. It may be worth defining broad security levels.
Security measures	For each confidentiality level it may be worth setting out the broad security measures to be followed, such as password protection, clear desk policy, entry control.
Business continuity	This would include backup procedures (both for data and for key staff availability) and emergency planning.
Specific risks	It may be worth setting out special precautions to be taken when information is in particularly risky situations, such as being worked on at home, with clients, at meetings, etc. It may also be worth addressing "social engineering" where staff are tricked into giving away information – for example, if a company calls posing as a supplement or herbal supplier and asks you to confirm a person's details. It would be good to label specific risks and include tactics for dealing with persistent requests for information over the phone, for example, or tips on dealing with the various e-mail risks may be worth considering. Common situations which may be worth mentioning include whether staff contact details may be given over the phone
Personal safety	A full security policy must also address personal safety of staff, including lone working.

Data recording and storage	
Accuracy	It may worth setting out measures to ensure data accuracy (or to refer to a separate case recording policy if this is more appropriate). For example, where information is taken over the telephone, how is it checked back with the individual? If information is supplied by a third party, what steps will be taken to ensure or check its accuracy?
Updating	If there is a regular cycle of checking, updating or discarding old data, this should be mentioned.
Storage	If there are particular considerations about where specific information should be stored, this could be mentioned. If your files are paper files, they would need to be stored in a secure place, under lock and key with limited access. If you are storing data digitally (such as digital intake forms, digital case taking forms, or any photographs of eyes) then the service provider you use should have a robust data security policy that should be included and referenced in your policy.
Retention periods	It may be worth setting out retention periods for different types of data. This would need to state how long you would hold
Archiving	The procedure for archiving or destroying data could be mentioned, along with any special considerations.

Subject access	
Responsibility	It may be worth reiterating who is responsible for ensuring that subject access requests (see notes) are handled within the legal time limit of 40 days.
Procedure for making request	Subject access requests must be in writing. It may be worth providing a standard request form (although its use cannot be made mandatory). There should be a clear responsibility on all staff to pass on anything which might be a subject access request to the appropriate person without delay. It is probably not useful to go into detail on the subject access procedure in the policy. Requests are infrequent and can be complex. They may require taking legal advice.
Provision for verifying identity	Where the person managing the access procedure does not know the individual personally there should be provision for checking their identity before handing over any information.
Charging	The organisation must spell out whether it charges for subject access (or access by some types of Data Subject). (The maximum fee which may be charged is £10.) If there is a charge, there must be a procedure for telling the Data Subject this when they make an access request.
Procedure for granting access	The normal provision is for the required information to be provided "in permanent form". If the organisation is willing to allow supervised access in person, this could be stated.
Transparency	
Commitment	The organisation may want to spell out its commitment to ensuring that in principle Data Subjects are aware that their data is being processed and • for what purpose it is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data Note that there is no obligation to inform people of anything that is obvious from the context or from general knowledge, or to inform people whose data is obtained from a third party where the cost of informing them would be disproportionate to the risks of holding and using the data: a typical example might be business contact lists.
Procedure	If there are standard ways for each type of Data Subject to be informed, these could be given, for example: • the handbook for staff • in the welcome letter or pack for members, with occasional reminders in the newsletter • during the initial interview with clients • on the web site
Responsibility	If different teams or staff members are responsible for transparency in relation to different types of Data Subject it might be worth indicating this.
Consent	
Underlying principles	Consent from the individual is one way of complying with the Fair Processing Conditions (see notes). It may be worth spelling out the situations, Data Subjects or types of data where the organisation will process data: • only with consent • preferably with consent, provided seeking it is practicable

	• without seeking consent Where data is being processed without consent it is still very important to ensure that the Data Subject knows what is being done.
Forms of consent	It may be worth specifying whether consent must be given in writing, or whether the organisation will accept verbal consent — and if so whether the giving of consent will be documented in any way.
Opting out	Even where the organisation is not relying on consent, it may wish to give people the opportunity to opt out of their data being used in particular ways (in addition to the right to opt out of direct marketing — see below).
Withdrawing consent	The organisation may wish to acknowledge that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.
Direct marketing	
Underlying principles	Although the Act does not define direct marketing clearly enough to be certain whether it incorporates many of the activities of voluntary organisations, good practice suggests that most unsolicited direct contact with individuals should be treated as marketing. This would include seeking donations, marketing goods and services, promoting sponsored events, raffles, etc. It is worth spelling out the activities which you will apply the marketing principles to.
Opting out	Because Data Subjects have the right to require their data not to be used for marketing, it is good practice to make it clear when there is an intention to use their data for marketing and offer them an opt-out (via a tick-box or an easy-to-use alternative) at the earliest opportunity. It may be worth setting out this principle, and also a procedure for ensuring that preferences are accurately recorded, and shared with all in the organisation who need to be able to act on them.
Sharing lists	Where lists are shared or exchanged with other organisations in order to carry out marketing-type activities, Data Subjects should be given an opt-out from their details being shared. It is worth committing the organisation to obtaining lists only where it can be guaranteed that those on the list have been given an opportunity to opt out, and also lists which can be guaranteed to be sufficiently up to date.
Electronic contact	Because of the Data Protection and Privacy (EC Directive) Regulations 2003 most electronic marketing (by phone, fax, e-mail or text message) either requires consent in advance, or it is good practice (and administratively easier) to obtain consent.

Staff training & acceptance of responsibilities	
Documentation	If procedures relating to Data Protection are maintained in addition to the overall policy, it may be worth listing them.
Other related policies	If other policies have a Data Protection content (such as those suggested above), it may be worth listing them.
Induction	All staff who have access to any kind of personal data should have their responsibilities outlined during their induction procedures.
Continuing training	If there are opportunities to raise Data Protection issues during staff training, team meetings, supervisions, etc, this may be worth mentioning.
Procedure for staff signifying acceptance of policy	Some thought should be given as to what staff are going to be asked to sign up to. This policy? Or the procedures in their own team or department?

Policy review	
Responsibility	It may be worth reiterating who has responsibility for carrying out the next policy review.
Procedure	It may be worth spelling out how other staff (and which staff) will be consulted in the review.
Timing	It may be worth setting out when the review has to be started, in order to be completed by the required date.

Notes

Data Controller

The Data Controller is the legal 'person' responsible for complying with the Data Protection Act. It will almost always be the organisation, not an individual staff member or volunteer. Separate organisations (for example a charity and its trading company) are separate Data Controllers. Where organisations work in close partnership it may not be easy to identify the Data Controller. If in doubt, seek guidance from the Information Commissioner.

Data Processor

When work is outsourced, which involves the contracting organisation in having access to personal data, there must be a suitable written contract in place, paying particular attention to security. The Data Controller remains responsible for any breach of Data Protection brought about by the Data Processor.

Fair processing conditions

Schedule 2 of the Data Protection Act lays down six conditions, at least one of which must be met, in order for any use of personal data to be fair. These are (in brief):

- With consent of the Data Subject
- If it is necessary for a contract involving the Data Subject
- To meet a legal obligation
- To protect the Data Subject's 'vital interests'
- In connection with government or other public functions
- In the Data Controller's 'legitimate interests' provided the Data Subject's interests are not infringed

Notification

All Data Controllers have to consider whether they are exempt from Notification. If they are not exempt, they have to Notify. This means completing a form for the Information Commissioner, and paying a fee of £35 a year. The Notification form covers:

- The purposes for which personal data is held (from a standard list) and for each purpose (again from standard lists):
- The types of Data Subject about whom data is held
- The types of information that are held
- The types of disclosure that are made
- Any transfers abroad

There is probably no need to mention the details of the organisation's Notification in the policy. The Notification entry has to be reviewed each year, and may have to change if the organisation changes its processing in significant ways.

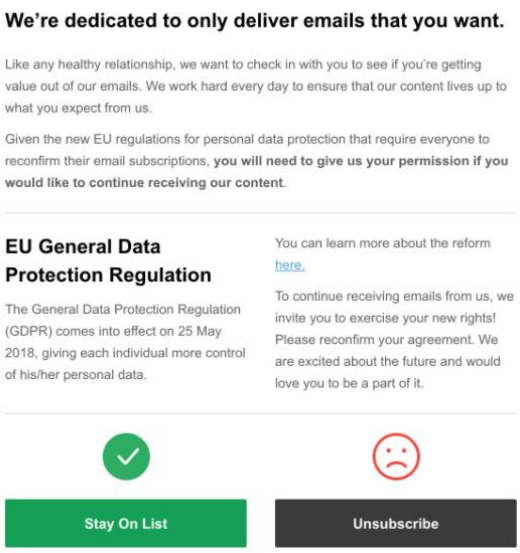
Subject access

Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request (including the fee, if required), the Data Controller must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made. The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld. This includes some third party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third Party" means either that the data is about someone else, or someone else is the source.)

Email opt in process

It is a good idea to email your data base and ask them to opt in to receiving further emails from you.

Your email service provider should have a data protection double opt-in template ready for you. Here is an example of what such a template may look like:



Payment processing and financial data

Your payment process will have their own policy on how financial data is handled and stored. Good practice would be to contact them and ask them what their data protection policy is, and include links to their policy in your own policy.

Example wording would be: “financial data is processed by PayPal. Payments processed by PayPal are subject to PayPal’s data protection policy. [link]”

Privacy Policy

The key areas pertaining to the new legislation is:

1. Right to be forgotten gives someone the power to ask a company to delete ALL of the data that is associated with that person. This requires you to provide more than an unsubscribe button. If a user makes a request, you must delete all the data stored in your databases and anything else associated with the user.

   You can refuse this request under special interest circumstances, such as where the information you keep is in the interest of public safety. For health data, the law requires you keep this for a period of 7 years, so you can archive the data instead of deleting it.

2. Right of access allows your subscribers to ask exactly how you are using their data and for what purposes. If a request is made, you’ll need to provide a personal data report at no cost to them. You have 30 days to respond, and two months to comply.

3. Breach Notification is mandatory under the GDPR, which means you have 72 hours from becoming aware of the breach to notify customers.

4. Right of portability lets people request their data, which means you would need to download a file of all their data in a ‘commonly used and machine-readable format’.

If you are storing digital data on servers, your service provider should have appropriate security mechanisms in place to alert any breaches and offset attempts to access data. Many practitioners will not be processing data digitally, but if you do have any online forms or digital forms you will need to make sure they are appropriately secure and have the specifications required by GDPR regulations which are services such as Amazon Web Services or any cloud provider with recognised certifications and audits in PCI DSS Level 1 and securities. Speak to your software provider for more information on the security mechanisms they have in place for handling sensitive data.

Secure digital data handling services should have 24/7 infrastructure monitoring with immediate notification and recovery in place in the event of a data breach.

Manual files should be kept in a secure, locked area with limitations and policy around who can and cannot access files. You should also have a policy on what you will do in the event the files are stolen or accessed by an unauthorised person.

Registering with the ICO

All persons who handle and control data must name themselves as a data controller in their data protection and privacy policies and register directly with the ICO for a £60 fee: https://ico.org.uk/for-organisations/register/

More information

The ICO have helpfully produced information on data protection as it related to Health data specifically. This can be found here: https://ico.org.uk/for-organisations/health/

The ANP is a Professional Association that supports practitioners, we do not give legal advice. Anyone is who is concerned about compliance is advised to seek the advice of a qualified solicitor.