Data Protection Policy – Template

Policy information	
Organisation	The name of the organisation responsible as the Data Controller **"data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed**
Scope of policy	Does the policy apply to branches, overseas offices etc. which the Data Controller is responsible for or only part of the organisation named above? Do you have any Data Processors acting on your behalf? If so, you should name them here. **"data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.**
Policy operational date	See below. A policy should be reviewed every 2 years
Policy prepared by	This should be the organisation's Data Protection Officer. If you process sensitive data, it is mandatory to appoint a DPO
Date approved by Board/ Management Committee	It is important that the policy should be approved by a Board if you have one
Policy review date	It is probably sufficient to review a Data Protection policy every three years.

Introduction	
Purpose of policy	This should include the reason for the policy: • complying with the law • following good practice • protecting clients, staff and other individuals • protecting the organisation
Types of data	This is where it is important to highlight the data you control. Is it personal and/or sensitive? See the ICO website definitions for details. Remember good practice applies to all data, even if it is outside of GDPR regulations https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/
Policy statement	This should 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 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/) Please also note the information on individuals' rights which is another key change (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)
Key risks	This should identify the main risks within your organisation in two key areas: • information about data getting into the wrong hands, through poor security or inappropriate disclosure of information • individuals being harmed through data being inaccurate or insufficient

Responsibilities	
The Board / Company Directors	They have overall responsibility for ensuring that the organisation complies with its legal obligations.
Data Protection Officer	There is no "right" person for this to be. It should be a fairly senior person, at least. Their responsibilities include: • Briefing the Board on Data Protection responsibilities • 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	Depending on the size of your organisation, you may want to mention IT or Marketing for monitoring their own compliance with GDPR and reporting back to the DPO
Employees & 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 'employees' is used, this includes both paid employees and volunteers.)
Enforcement	You may want to say what the penalties are for infringing the Data Protection and related policies. You should state what training you provide and what methods of reporting you have internally.

Security	
Scope	Data Security is not wholly a Data Protection issue. Business Continuity is included below but you may want to move this to a separate policy
Setting security levels	The greater the consequences of a breach of confidentiality, the tighter the security should be
Security measures	For each confidentiality level it may be worth setting out the security measures to be followed, such as password protection, clear desk policy, entry control This section should include your technical and organisational security measures
Business continuity	This would include backup procedures (both for data and for key employee availability) and emergency planning. As noted above, it may be worth a separate policy
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 "vishing" and "phishing" where employees are tricked into giving away information over the phone or by email. Tactics for dealing with the risks of both are worth including Common situations which may be worth mentioning include whether contact details may be given over the phone

Data recording and storage	
Accuracy	It may worth setting out measures to ensure data accuracy. 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. Please note the separate requirements for the data you hold. For example, you cannot keep CVs for more than 6 months unless you have express permission from the candidates
Storage	If there are particular considerations about where specific information should be stored, this should be mentioned
Retention periods	It may be worth setting out retention periods for different types of data
Archiving	The procedure for archiving or destroying data should be mentioned, along with any special considerations (see above)

Right of Access	
Responsibility	It may be worth reiterating who is responsible for ensuring thatright 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. It may be worth providing a standard request form. There should be a clear responsibility on all employees 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 right of access procedure in the policy. Requests are infrequent and can be complex. They may require taking legal advice https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
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	You should provide the information free of charge. However you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information
Procedure for granting access	If the request is made electronically, you should provide the information in a commonly used electronic format. The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. This will not be appropriate for all organisations, but there are some sectors where this may work well

Transparency	
Commitment	The organisation should explain its commitment to ensuring that 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
Procedure	If there are standard ways for each type of Data Subject to be informed, these could be given, for example: • the handbook for employees • 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 employees are responsible for transparency in relation to different types of Data Subject it might be worth indicating this

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/) Personal data shall be: a. processed lawfully, fairly and in a transparent manner in relation to individuals; b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
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
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

Employee training & Acceptance of responsibilities	
Induction	All employees 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 employee training, team meetings, supervisions, etc. this may be worth mentioning
Procedure for staff signifying acceptance of policy	Give thought to how employees will show acceptance of their responsibilities to Data Protection. Will the policy be included in the Company Handbook etc.?

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 employees (and which ones) 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

When using a third party data processor, please read the guidelines here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/