# **Data Protection Policy – Sample**

|  |  |
| --- | --- |
| Author:  |  |
| Adopted by (e.g. Management Committee) | Date |
| Review date:  |  |

**Introduction**

The General Data Protection Regulation (GDPR) is an EU law that took effect on 25 May 2018 and is likely to become law in the UK after transition out of the EU. Data Protection regulation applies to all organisations that hold any information that identifies living people. This Data Protection Policy has been produced to meet GDPR requirements. The Information Commissioner’s Office (ICO) enforces GDPR in the UK. Fines are up to $20m or 4% of turnover whichever is the greatest.

**Commitment**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is committed to fully complying with GDPR rules. This means that every person involved in this group will observe this policy.

Formal Contact

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the Data Controller.

Contact address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**What is personal data?**

Personal data refers to any information which can be used to identify an individual directly or indirectly. This means any information we hold containing someone’s name, address, phone number, National Insurance number, photograph etc. in a way that identifies that individual constitutes personal data. That also includes reports, minutes or recordings of conversations in which we refer to an individual by name or in a way that could identify them. Examples would include an email address like jane.doe@abccharity.org.uk, because only one Jane Doe works at ABC Charity, or a comment about the CEO of ABC Charity, because that person can easily be identified indirectly. (Source ICO)

**On what bases may we process personal data?**

There are six lawful bases for the storage and use of individual data. We must be able to justify its data use according to one of the lawful bases.

In the words of the ICO guidelines these are:

**“(a) Consent:**the individual has given clear consent for you to process their personal data for a specific purpose.

**(b) Contract:**the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

**(c) Legal obligation:**the processing is necessary for you to comply with the law (not including contractual obligations).

**(d) Vital interests:**the processing is necessary to protect someone’s life.

**(e) Public task:**the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:**the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)”

**Data**

We gather, process, store and sometimes share personal data to enable the group to fulfil a range of purposes including:

* Administration and governance
* Organiser of events
* Fundraising
* Promoting the aims of the group
* Working with contractors and volunteers

**How we interpret the principles of GDPR**

The law is based on principles which means that we have to interpret these to decide how we collect and process our data. This policy cannot cover every eventuality.

**Code of Practice**

1. We **always make it clear** to the individual why we are collecting their personal data.
2. We collect personal data **only to carry out our group activities**.
3. We keep personal data **up to date and accurate**.
4. We regularly review our records and **delete any personal data that is no longer needed**, or we redact (remove) personal data.
5. We can **archive** personal data **when there is a legitimate reason to do so**.
6. We **never share** personal data outside the group, unless for reasons that were transparent when the data was collected.
7. **Consents**

**i.** **Individuals always understand** what their data will be used for, and give clear consent, and we store their consent

**ii. Consent is explicit and opt in**. Sometimes consent is clearly implied, for example, when someone gives their email address for a newsletter, or provides telephone contact information for a specific purpose. They know what purposes the data will be used for, and we don’t need to ask them to sign an additional consent form. At other times, specific consent is needed to make it clear to the individual, particularly regarding the use of images (see below).

**iii. We obtain specific ‘granular’ consent for the use of photographs, films or quotations** that identify an individual. ‘Granular’ means that individuals can opt in to specific uses (usually in a tick box format) over a stated period of time.

**iv. We store** consents securely.

1. **Safe and Secure**

We make sure that all personal data is protected by passwords (online) or in locked cupboards and that we have processes in place to safeguard the data.

1. **Direct marketing**

Direct marketing refers to materials used to promote “aims and ideals”. This means that a newsletter, event invitations, and publicity for events all constitute direct marketing if they could be seen to promote our aims and ideals.

**i. Email**

We can send emails to a general business address e.g. info@school.co.uk without prior consent.

Individual recipients of emails, even if they are in their business/ work capacity e.g. MrSmith@business or school.co.uk must **opt in** before we send them direct marketing emails.

**ii. Post**

We can post direct marketing materials to an individual as long as we give them an opt-out option.

**iii. Phone**

We can phone individuals, unless they have opted out through the Telephone Preference Service.

1. **Unsubscribe**

We always include an **unsubscribe/ opt out** option on all our direct marketing communications.

1. **Data breaches and reporting**

“A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.” (Source - ICO)

1. **Subject Access Requests**

We make it clear to individuals how to request information about the personal data held by us, and we provide individuals with the personal data that we hold about them within one month of their request and sooner if possible.

1. **Data Retention**

We regularly review data, and archive, update or delete as appropriate.

1. **Review**

We check that records are compliant once a year

**Social media**

* We have granular\*, time-limited, consent for all photographs and films that show individuals.
* A Privacy Policy is linked from our social media accounts.
* We do not share social media posts that identify individuals unless we have specific consents from the individuals.

**Emails**

* We use the BCC function to hide individual email addresses when contacting groups.
* We delete emails on an on-going basis.
* We archive emails every six months.

**Communication by Post**

* When we direct market to a named individual we give the recipient an easy option to unsubscribe.

**Photographs and films**

Featuring Individuals

* We have granular\* opt in consent (from the parent/guardian of pupils up to 16 years old, and from the pupil when aged 16 and over) to store and use photographs and film that feature individuals on;
	+ Social media
	+ For media
	+ For any other use

Featuring groups (that don’t single out individuals)

* We obtain consent, signed by a teacher or lead person, that confirms that individual consents have been obtained.
* We store records of consent securely
* We let people choose what they opt in to.
* We make it easy for people to opt out if they want to.

**Contact Mailing Lists**

* Contact addresses are kept in mailing lists and kept for mailing purposes and password protected.

**\*Granular** means that individuals opt-in for each kind of use that the photograph or film will be used for. They may opt in for a period of time.

**Questions**

Any questions or comments about this data protection policy should be addressed to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_