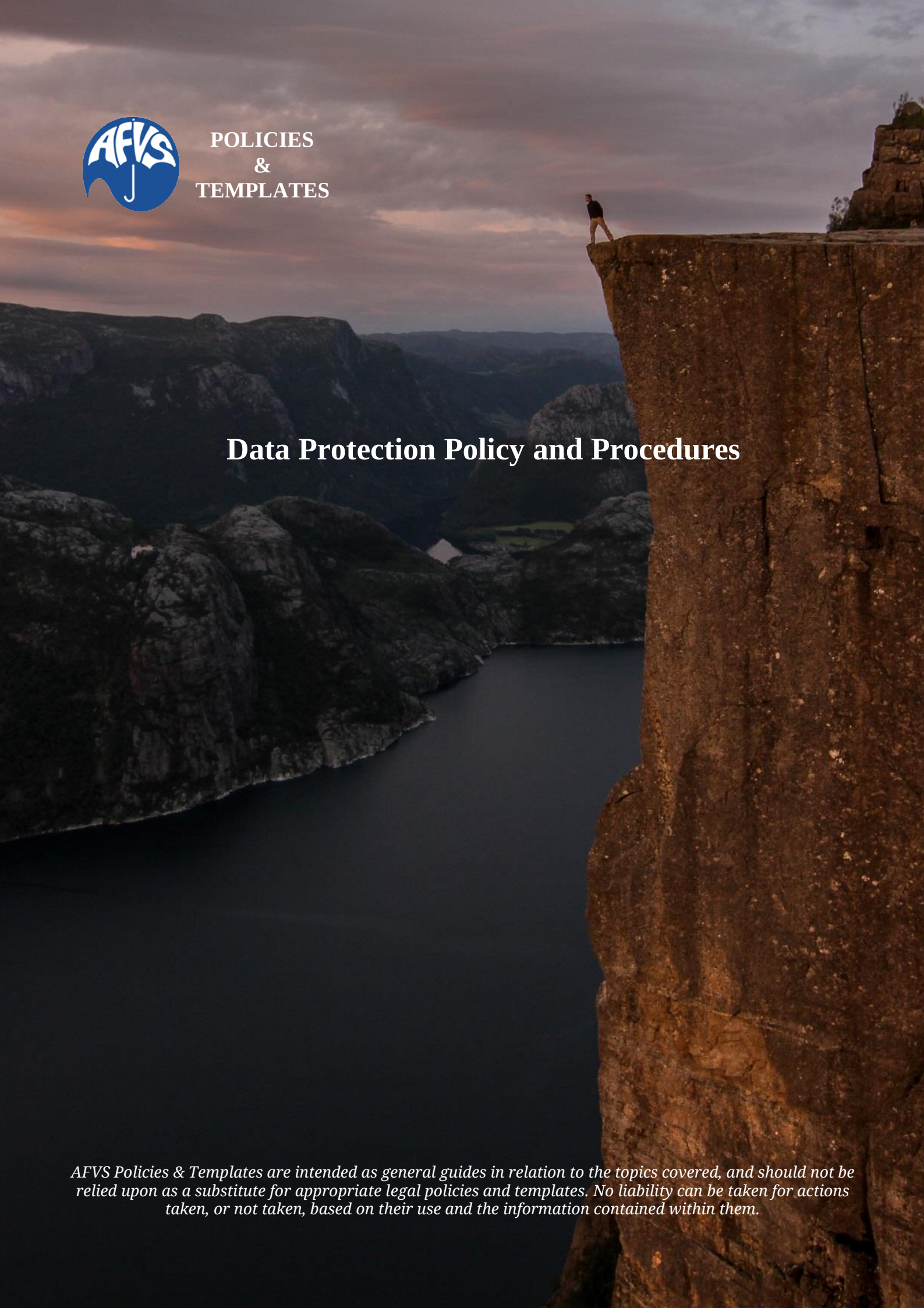

POLICIES
&
TEMPLATES

Data Protection Policy and Procedures

Introduction

As I write this introduction, I just called up a news report I sent out on Twitter last week; 11 charities have received fines ranging from £6,000 to £18,000. The Regulator wanted the fines to be higher given the gravity of the offences, but being mindful that these fines would come out of the pockets of donors, kept them low. It gets worse; the Charity Commission is now weighing in by making their own investigations into the offending charities. At least one charity is complaining about it being unfair; the others are, I suspect, getting their systems and practices overhauled.

The Fundraising Regulators Code of Conduct runs to almost 80 pages, with regular updates coming out. I have summarised it down to a dozen or so pages, still 5,500 words to get to grips with. You can find a copy of our summary on our website. We have included a Complaints Policy template in the Appendix. As a trustee or administrator, you need a working understanding of the Code and how it affects your charity. I also recommend you register with the Regulator. It is voluntary, but will put you in a better light if you do get a complaint against you.

Very important points to remember:

1. Do not ever forget that data subjects have the legal right to see every reference to them that you have stored in your records (there are some opt outs in the small print, but nothing you should rely on). Do not ever put anything in writing that you would not wish them to see. (Charities are not covered under the Freedom of Information Act, but are covered under Data Protection law.)

2. Remember that your policy should include information stored on personal laptops, home computers and Smartphones. Policing them can be very difficult, so it is important that your team of staff and volunteers are well trained and well briefed.

This is a Data Protection Policy template, taken from the HMRC website.

(Name of Charity)

Data Protection Policy and Procedures

Introduction
We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Data in order to carry on our work. This personal information must be collected and dealt with appropriately.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data).

Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The charity will remain the data controller for the information held. The board, staff and volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act.

Board members staff and volunteers who have access to personal information, will be expected to read and comply with this policy.

Purpose
The purpose of this policy is to set out the [charity] commitment and procedures for protecting personal data. The board regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

The Data Protection Act Legislation
This contains 8 principles for processing personal data with which we must comply.

Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

3. Shall be adequate, relevant and not excessive in relation to those purpose(s),

4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary,

6. Shall be processed in accordance with the rights of data subjects under the Act,

7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:

Data Controller – The person who (either alone or with others) decides what personal information [Group] will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person on the management committee who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998.

Data Subject/Service User – The individual whose personal information is being held or processed by [Group] (for example: a service user or a supporter)
'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him.

Explicit consent is needed for processing sensitive data this includes the following:

(a) racial or ethnic origin of the data subject
(b) political opinions
(c) religious beliefs or other beliefs of a similar nature
(d) trade union membership
(e) physical or mental health or condition
(f) sexual orientation

(g) criminal record
(h) proceedings for any offence committed or alleged to have been committed

Notification – Notifying the Information Commissioners Office (ICO) about the data processing activities of the [Group]. Note: Not-for-profit organisations are exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of the Group.

Applying the Data Protection Act within the charity
Whilst access to personal information is limited to the staff and volunteers, Volunteers may undertake additional tasks which involve the collection of personal details from members of the public.

In such circumstances, we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

Correcting data
Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress or to stop marketing information being sent to them.

Responsibilities
The [charity] is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

The management committee will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

a) Observe fully conditions regarding the fair collection and use of information.
b) Meet its legal obligations to specify the purposes for which information is used.
c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
d) Ensure the quality of information used.
e) Ensure that the rights of people about whom information is held, can be fully exercised under the Act.
These include:
i) The right to be informed that processing is being undertaken
ii) The right of access to one's personal information
iii) The right to prevent processing in certain circumstances, and
iv) The right to correct, rectify, block or erase information which is regarded as wrong information
f) Take appropriate technical and organisational security measures to safeguard personal information,
g) Ensure that personal information is not transferred abroad without suitable safeguards,
h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
i) Set out clear procedures for responding to requests for information.

The Data Protection Officer on the management committee is:

Name _____

Contact Details _____

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice
b) Everyone processing personal information is appropriately trained to do so
c) Everyone processing personal information is appropriately supervised
d) Anybody wanting to make enquiries about handling personal information knows what to do
e) Dealing promptly and courteously with any enquiries about handling personal information
f) Describe clearly how the charity handles personal information

g) Will regularly review and audit the ways it holds, manages and uses personal information
h) Will regularly assess and evaluate its methods and performance in relation to handling personal information

All staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

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 made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

Data collection: Informed consent

Informed consent is when a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent.

We will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, we will ensure that the Data Subject:

a) Clearly understands why the information is needed
b) Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
e) Has received sufficient information on why their data is needed and how it will be used

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is our responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

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 made to the Data Protection Act 1998.

Data Subject Access Requests
Members of the public may request certain information from public bodies under the Freedom of Information Act 2000. The Act does not apply to charities, but we are still required to respond to requests for information under the Data Protection laws.

Disclosure
We may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person
b) The Data Subject has already made the information public
c) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
d) Monitoring for equal opportunities purposes – i.e. race, disability or religion
e) Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

We intend to ensure that personal information is treated lawfully and correctly.

Risk Management
The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

Destroying personal data.
Personal data should only be kept for as long as it is needed i.e. only keep that data for the duration of administering the campaign/project and securely dispose of once the promotion and monitoring period is complete. If a customer is housebound and receives regular visits from a volunteer – ensure the list is securely stored and remove customer details when they change or the customer no longer receives the service. We will review the list annually, and will ensure that this information is confidentially destroyed at the end of the relevant retention period.

Further information
If members of the public/or stakeholders have specific questions about information security and data protection in relation to the charity please contact the Data Protection Officer:

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.

By Daryl Martin
March 2017