1. Data Protection Policy

Version	Action	Date	Signed
DRAFT B	Created	09/07/2021	C D Compton
	Authorised		

2. Introduction

a. Totton & Eling Community Association (TAECA) needs to keep certain information about its employees, trustees, volunteers, members, clients and other members of the public to enable it to monitor performance and achievements. It is also necessary to process information so that staff can be recruited and paid, activities organised and legal obligations to funding bodies and government fulfilled.

b. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Totton & Eling Community Association must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the Act). In summary these state that personal data must be:

   i. obtained and processed fairly and lawfully;
   ii. obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose;
   iii. adequate, relevant and not excessive for that purpose;
   iv. accurate and kept up to date;
   v. not be kept for longer than is necessary;
   vi. processed in accordance with the data subject's rights;
   vii. kept safe from unauthorised access, accidental loss or destruction; and
   viii. not be transferred to a country outside the UK.

c. All Totton & Eling Community Association staff and volunteers who process or use any Personal Information must ensure that they follow these principles at all times.

d. Any member of staff, trustee or volunteer, who considers that this policy has not been followed in respect of personal data about him/herself, should raise the matter with the Designated Data Controller initially. If the matter is not resolved, it should be raised as a formal grievance.

3. Notification of Data Held and Processed

a. All employees, trustees, volunteers, members, clients and other members of the public have the right to:
    i. know what information Totton & Eling Community Association holds and processes about them and why;
    ii. know how to gain access to it;
    iii. know how to keep it up to date; and
    iv. know what TAECA is doing to comply with its obligations under the Act.

4. The Data Controller and the Designated Data Controllers

a. Totton & Eling Community Association as a Charity is the Data Controller under the Act, and the organisation is therefore ultimately responsible for implementation. However, Designated Data Controllers will deal with day to day matters.
b. The TAECA Designated Data Controllers are the Centre Administrators.

5. Information Held

a. Personal Information is defined as any details relating to a living, identifiable individual. Within Totton & Eling Community Association this applies to employees, trustees, volunteers, members, clients and other members of the public such as job applicants and visitors. We need to ensure that information relating to all these people is treated correctly and with the appropriate degree of confidentiality.
b. Totton & Eling Community Association holds Personal Information in respect of its employees, trustees, volunteers, members, clients and other members of the public. The information held may include an individual's name, postal, e-mail and other addresses, telephone and facsimile numbers, subscription details, organisational roles and membership status.
c. Personal Information is kept in order to enable Totton & Eling Community Association to understand the history and activities of individuals or organisations within the voluntary and community sector and to effectively deliver services to its members and clients.
d. Some Personal Information is defined as Sensitive Data and needs to be handled with special care (see paragraph 10. below).

6. Processing of Personal Information

a. All staff and volunteers who process or use any Personal Information are responsible for ensuring that:
    i. Any Personal Information which they hold is kept securely; and

ii. Personal Information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

b. Staff and volunteers should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.
   i. Personal information should be:
   ii. kept in a locked filing cabinet; or
   iii. in a locked drawer; or
   iv. if it is electronic, be encrypted; or
   v. stored only on a device which is itself secure.

7. Telephone Conversations and Meetings

a. If personal information is collected by telephone, callers should be advised what that information will be used for and what their rights are according to the Act.

b. Personal or confidential information should preferably not be discussed in public areas of Totton & Eling Community Association's work premises or within open-plan office areas. Wherever possible, visitors should be escorted to a private interview room or office and not be permitted to wander about the premises on their own. If possible, visitors should subsequently be escorted out of the premises when the meeting is over. All staff should be aware of the difficulties of ensuring confidentiality in an open plan area and respect the confidential nature of any information inadvertently overheard. Any notes taken during or after an interview should be of relevance and appropriate. It is recommended that such notes are subsequently filed in a legible and coherent manner and that informal notes are retained for a short period (1 year), in a secure place, before being shredded.

8. Collecting Information

a. Whenever information is collected about people, they should be informed why the information is being collected, who will be able to access it and for what purposes it will be used. The individual concerned must agree that he or she understands and gives permission for the declared processing to take place, or it must be necessary for the legitimate business of Totton & Eling Community Association.

9. Publication and Use of Totton & Eling Community Association Information

a. Totton & Eling Community Association aims to make as much information public as is legally possible. In particular information

about staff, trustees and members will be used in the following circumstances:

b. Totton & Eling Community Association may
   i. obtain, hold, process, use and disclose information in connection with the administration, management and business activities of Totton & Eling Community Association, including making and keeping lists of members and other relevant organisations.
   ii. publish information about the organisation and its members including lists of members, by means of newsletters or other publications.
   iii. confirm to any third party whether or not any person is a member of Totton & Eling Community Association.
   iv. provide approved organisations with lists of names and contact details of members or other relevant organisations only where the members or other relevant organisations have given their consent.
   v. use information for anything ancillary or incidental to any of the foregoing.
   vi. may publish names of, and a means of contacting, staff and trustees within publicity leaflets and on the website.
   vii. Display photographs of key staff at Totton & Eling Community Association or placed on the website with their consent.
c. Totton & Eling Community Association's internal staff contact list will not be a public document and information such as mobile telephone numbers or home contact details will not be given out, unless prior agreement has been secured with the staff member in question.
d. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Centre Administrators (Designated Data Controllers).

10. Sensitive Information

a. Sensitive information is defined by the Act as that relating to ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sexual orientation, criminal proceedings or convictions. The person about whom this data is being kept must give express consent to the processing of such data, except where the data processing is required by law for employment purposes or to protect the vital interests of the person or a third party.

11. Disposal of Sensitive Material

a. Sensitive material should be shredded. Care should be taken to delete data from computer hard drives if a machine is to be disposed of or passed on to another member of staff. See ICT policy for operational procedures on the retention and disposal of electronic data.

12. Staff Responsibilities

a. All staff are responsible for checking that any information that they provide to Totton & Eling Community Association in connection with their employment is accurate and up to date. Staff have the right to access any personal data that is being kept about them either on computer or in manual filing systems.
b. Staff should be aware of and follow this policy, and seek further guidance where necessary.

13. Duty to Report

a. There is a legal duty to disclose certain information, namely, information about:
    i. Child abuse, which will be disclosed to social services; or
    ii. Drug trafficking, money laundering or acts of terrorism or treason, which will be disclosed to the police.
    iii. Loss of personal information to the Information Commissioners Office (ICO) where a breach is likely to result in a risk to the rights and freedoms of individuals.

14. Retention of Data

a. Totton & Eling Community Association will keep some forms of information for longer than others. In general information about clients will be kept for 'no longer than is necessary' this is considered to be up to three years after they use Totton & Eling Community Association services, unless other bodies, such as funders, require Totton & Eling Community Association to keep the information longer in which case the individuals concerned will be informed.
b. Totton & Eling Community Association will also need to retain information about staff. In general, all information will be kept for six years after a member of staff leaves the organisation. Some information however will be kept for much longer, for example, if required by funders. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for

job references. A full list of information with retention times is included in the Retention and Disposal Policy.

15. Notification

a. A statement about Data Protection will be displayed clearly within public spaces within TAECA's premises and on the website. A copy of our privacy statement is available on our website.

NOTES ----------

GDPR for Committees and Staff Members of Charities and Community Groups

GDPR is the new buzz word – due to take effect from 25th May 2018. GDPR means General Data Protection Regulations. It is new UK law, derived from EU law, and updates the regulations under the Data Protection Act 1998 (DPA).
In most aspects if your organisation was fully compliant with the regulations under the DPA then little more will be needed. But you will need to review and assess compliance, even if yours is a very small organisation.
The reason behind introducing the new regulations is because the way personal data is processed has changed dramatically over the last 20 years. Technological change is the biggest change but also there are changes in the way data is used for commercial purposes, for charitable fund raising and for data coordination and sharing.
The Eight Data Protection Principles remain at the heart of the regulations
data must be:

1. Fairly and lawfully processed;
2. Processed for limited purposes;
3. Adequate, relevant and not excessive;
4. Accurate;
5. Not kept for longer than necessary;
6. Processed in line with your rights;
7. Secure, and;
8. Not transferred to countries without adequate protection;

GDPR makes “Privacy by design” an express legal requirement. Therefore any charity or community group that records people’s name and any more information must consider the Data Protection requirements.

Summary simple rules for simple situations

The committee of any group that has computer records or even paper records of their members or beneficiaries are legally obliged to consider why they keep the data, that it only be used with consent of the person in the way(s) agreed and that it is kept secure and private. Committees of community groups and charities must get help if they do not know what to do to meet the GDPR requirements. There are legal justifications for processing data; the group needs to determine which applies to them. See appendix
This information has been compiled by Communities First Wessex, Community Action Fareham and Gosport Voluntary Action working together to better share resources and expertise for benefit of our member groups.

 Personal data must always be processed fairly, handled for intended purpose and only in ways that an individual would reasonably expect. Obtain and keep record of consent
 Don't download data to laptops or pen drives without password encryption
 Don't send data files by email unless absolutely necessary
 Maintain confidentiality on need to know basis
 Train all staff, including volunteers, and obtain confidentiality agreement
 Delete or destroy securely when no longer required

Some Definitions
Personal Information is data about any living person. This applies to paper records and those on computers. It would include computer IP addresses and internet cookies.
Sensitive Personal Information (under GDPR called Special Categories) would include data about:
 Race or ethnic origin
 Political opinions
 Religious or similar beliefs
 Being a member of a trade union
 About the physical or mental health
 About sexual life
 About offences
 This also includes biometric and genetic data such as DNA or fingerprints

The Data Controller is the organisation (or person) who decided the purposes for which and the manner in which any personal data are, or are to be, processed.
The term **"Data Processing"** is central to everyone's understanding of the subject. It includes anything done with data including the fact that it remains on a computer without anyone accessing it. It refers to deleting it. It includes everything about how it is accessed, changed or compiled. The data processor is the organisation or person undertaking the processing. It may be a contractor on behalf of the data controller. There must be a formal contract between the Data Controller and any external Data Processors
Data Subject is the term referring to the person whose information / data is held.
Subject Access is the provision for the person to be provided with all the information about themselves.
Breaches of data must be reported to the UK regulator – the Information Commissioners Office (ICO). It must also be reported to the Charity Commission as a serious incident.
Note that under GDPR, the ICO has power to issue higher fines. This is up to €20m or 4% of turnover.
Organisational Data is not subject to DPA or GDPR as it is not in relation to a living person. So the contacts at an organisation using the organisations domain is not personal data. However many community groups are so small that their contact details would be the same as their personal contact details and so DPA and GDPR apply to

them This information has been compiled by Communities First Wessex, Community Action Fareham and Gosport Voluntary Action working together to better share resources and expertise for benefit of our member groups.

For Charities and Community Groups

1. You must design your DP policy and procedure to suit the data processing requirements of the organisation. Therefore your board of trustees or Committee must have examined the requirements of GDPR and have taken a decision in how they will process personal data. The way this would be seen is if there is a Data Protection policy.

2. If handling beneficiary data then it may be necessary to register with the ICO.

3. People must give consent to their data being processed. The consent must be clear, recorded and be able to be withdrawn. Data Controllers must be able to demonstrate that they have been given consent.

4. People have the right to have all their data removed; this is called 'the right to be forgotten'.

5. If people's data is given to another organisation, eg Payroll or Pensions or other service, then there must be a binding contract between the data controller and the contracting processor.

6. Staff, employees and volunteers, will need training. It will be necessary for them to declare compliance with policy. This would normally be by signing a Confidentiality and Data Protection Agreement.

Complying with Good Practice

 Have a Data Protection Policy that has been updated for GDPR.

 Undertake a Data Protection audit to identify extent and use of personal data

 Data security policy and procedures that enable data to be kept securely and safe. Therefore firewalls, anti-virus and passwords must be good. Data must be kept up to date and regularly backed-up.

 Evidence of data subject consent to handling data. For employees this will include passing of relevant information to contractors for payroll, pensions and other employment processes.

 Evidence of training for all staff who handle data, including any more than knowing the name of someone in the charity. (unrecorded personal conversations are not included).

 Evidence of staff agreement of understanding and to comply with the policy and procedures.

 Data can be processed if there is "legitimate interests" – such as holding employee or membership information.

 Data can be shared if it is in the "Vital Interests" of the person – such as with a hospital emergency department after an accident.

Data Protection Officer

A Data Protection Officer (DPO) must be appointed in certain circumstances. This is for public organisations like councils or the NHS, or when there are data subjects who are monitored on a large scale or when a large amount of sensitive personal data is handled –sensitive data would include any criminal records information. The DPO must be a senior person reporting at the highest level. They must have independence to undertake their audit responsibilities. This information has been compiled by Communities First

Wessex, Community Action Fareham and Gosport Voluntary Action working together to better share resources and expertise for benefit of our member groups.

Most small charities and community groups would not have to appoint a DPO. However the committee may wish to appoint a lead person who is well trained in Data Protection and GDPR. Committees that are unsure about GDPR must (according to the Charities Commission) ask for help. Help is available from Community Action Fareham.

The fines for non-compliance are now much higher. Two new offences under GDPR include re-identifying individuals from anonymised data and altering personal data to prevent disclosure such as after a Subject Access Request (SAR)

Fundraising

Using databases of supporters, donors and members for fundraising purposes requires special consideration under the regulations. Consent to the charity holding the information, consent to be sent fundraising communications in specific ways and the right to change or cease must be included.

It has been and will continue to be an offence to manipulate data and share data. RSPCA and BHF were fined £43,000 in 2016 and 11 more in 2017 were fined a total of £138,000. They had been carrying out processing contrary to Data Protection Act regulations including:

- “wealth screening” – identifying people from various sources according to their wealth
- obtaining data from other sources to add to their own data bases – “data matching”
- and sharing the data with other charities without the donor’s consent.

This illustrates that the collection and use of data must be transparent and only used for the declared purposes.

If you use personal data for fundraising and your costs of fundraising are over £100k per year you are expected to register and pay a levy. Guidance about fundraising is on the regulator’s website www.fundraisingregulator.org.uk

Email newsletters and campaigns

People must only be sent email newsletters or promotions to their personal addresses if they have specifically signed up to receiving information from you. They have a right to be removed effectively from your list, and “to be forgotten”. It is expected practice that all emails will provide the “From” address, the organisations details and an option to be removed from the mailing list.

If organisations have email lists without a record of consent to join it then, for personal email addresses, the consent must be renewed. If there is no response it’s a no!

Emails sent to lists of people must always be sent blind copied unless you have express permission to show the distribution – eg for a committee or internal at work. This information has been compiled by Communities First Wessex, Community Action Fareham and Gosport Voluntary Action working together to better share resources and expertise for benefit of our member groups.

Data Protection & Privacy Statement

All forms that collect people's name and information, for either an ongoing membership purpose or a one off event record must have a Data Protection Statement. There should also be a tick for consent to process the data – that would include keeping the paper form and transferring the data to a computer as well as any other ongoing use. The statement must say how the data will be used, to add to an email distribution list or to share the data. The consent must be clearly given for the specific purposes.

Privacy notes may be separate and have more detailed content.

Example / Model statement

The information given will be added to a computer system for the purposes of maintaining our membership administration. Please tick the boxes below to give your consent to how we will communicate with you and use your personal information.

I give consent to my information being kept on [organisation]'s systems for administration of membership

I give consent to receive mail and emails about the programme and news

I give consent to my information being passed to partner organisations who may have products or programmes of potential interest

The above shows the form that a statement may take. It would have to suit the requirements of the organisation. You don't have to ask irrelevant questions.

Four technical aspects for the organisation's Committee and Data Protection lead.

Subject Access requests (SAR)

Individuals are entitled to ask for a full record of data held about them. They must be provided with this within 1 month. They can no longer be charged. The information required to be provided is anything that is "Biographical". A document has to have a specific reference to the data subject. Therefore this does not include a name or a passing reference to the person in a report or email.

It is important that when a Subject Access request is made, that the request is verified to come from the data subject. There have been cases of people wanting to find out information held about others. This applies to information about children, when they are the data subject – the SAR must be given to the child and not the parent.

Subject Access requests can be refused or charged for if they are manifestly unfounded or excessive. This information has been compiled by Communities First Wessex, Community Action Fareham and Gosport Voluntary Action working together to better share resources and expertise for benefit of our member groups.

Document and file retention times; Organisations are required to keep certain information for either maximum or minimum times. Therefore this links to Data Protection. Any personal data must be kept securely for the whole period of the retention period then it must be disposed of securely.

Here is a selection of the more common document types that relate to voluntary organisations. Organisations may need to consider their document retention in further detail and create a policy. Committee minutes and decisions, annual accounts	At least 10 years, perhaps permanently
Records of a closed community group or charity	20 years
Bookkeeping records, invoices etc	6 years
Records of services	10 years
Correspondence	If contains personal information then maximum not longer than for lawful purposes in keeping it.
Employers Liability Insurance certificate	40 years
H&S records	3 years
Safeguarding or child attendance records (there will be a difference between simple registers, accident records, safeguarding concerns and investigations)	Depends, organisation must take advice and decide, perhaps for 3 years or until child is 18 or 25 or some say for 100 years
Accident reports	3 years
Contracts	10 years after completion
Employee records, payroll records, pension records	6 years
Sickness records	3 years
Employee work and rest periods	2 years min.
Maternity pay records	3 years
Unsuccessful job applicants	6 months