Saltford Business Network - Data Protection

The Data Protection Act 1998 ("DPA") has a number of requirements that must be met by any organisation that processes personal information. In particular it has regulations governing how an individual's personal information is used and to protect people from misuse of their personal details.
The definition of personal data covers any information through which a living individual is identifiable. It will include name, address, date of birth etc. and also use of CCTV and other images.
The definition of processing covers almost anything done with personal data/information including organising, adapting, amending, retrieving, consulting, using, disclosing, erasing, destroying and storing it.

Saltford Business Network collects information about business names, addresses, phone numbers, email etc that is already in the public domain which would not usually be covered by the DPA. However for small businesses run from home the information may also be sufficient to identify an individual so Saltford Business Network has developed and agreed the following Data Protection Policy and Procedures.

Data Protection Policy

This policy will ensure that Saltford Business Network will meet the requirements of the Data Protection Act 1998 by:

- Understanding the legal requirements of the Data Protection Act
- Complying with the eight data protection principles
- Making sure that queries about data protection are dealt with effectively and promptly
- Having an agreed set of procedures which are kept up to date by regularly reviewing them.

Sign Off on Policy

Name: Kevin Reeves **Position:** Chairman

Dated: 7th March 2013

We will review this policy and our procedures annually.

This policy was last reviewed on:

7th March 2013

Data Protection Procedures

Forms

- Forms used to collect data to be worded to ensure that all individuals give their explicit consent when they supply sensitive information or information which could be used for commercial purposes.
- Forms to be worded to give people a clear understanding of how the information they are providing could be used.
- We need to be clear about how/if any SBN information could be used for commercial purposes. For example it would not be appropriate for our mailing list to be used by an SBN member to market/ advertise a particular business or product.

Storing Information

- Paper records will only be retained by the Treasurer and the Membership Secretary, they will be stored securely and shredded when no longer required
- Only essential paper records to be stored e.g. copies of signed membership forms and financial records.
- Only one person at any time maintains the membership list.
- Only one person at any time maintains the email contact list.
- Only one person at any time maintains the list of members' financial details.
- All electronic lists to be stored either as a password protected excel spreadsheet or on a password protected computer.

Recording Information

When entering data that could identify an individual:

- Ensure personal data is entered accurately.
- Check what data protection consents have been given by the individual.
- If paper records exist they must be properly filed or disposed of when no longer needed.

When accessing and using data that could identify an individual:

- Check that the individual has consented to the planned use of this data.
- Don't access this data unless you have permission and you need it to do your job or role.
- Don't print out this data from computer files unless there is a good reason to do so.

Emails and other communication

When communicating with individuals:

- Check the individual has requested or consented to your communication.
- Ensure that any "commercial" communications SBN sends includes an opt-out.
- Make sure that any opt-outs are recorded and reported appropriately.
- Make it obvious that SBN is the sender of the communication.
- Take care over the content, suitability and frequency of communications.
- Don't use old mailing lists.
- Group emails, beyond the working group, to be sent with individual email addresses in BCC
- Be clear about how/if any SBN information could be used for commercial purposes. For example it would not be appropriate for our mailing list to be used by an SBN member to market/ advertise a particular business or product

Data Protection Supporting Information

The Law and Data Protection Principles

The Data Protection Act 1998 (DPA) gives individuals the right to know what information is held about them, and provides a framework to ensure that personal information is handled properly by organisations, businesses or the government. It also imposes restrictions on the transfer of data outside the European Economic Area, which has particular implications for placing material on the internet.

The Data Protection Principles

Organisations must comply with these eight principles which make sure that personal information is:
1. fairly and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;
4. accurate and up to date;
5. not kept for longer than is necessary;
6. processed in line with the rights of individuals;
7. secure; and
8. not transferred to other countries without adequate protection.

Notification and Exemption

As it is currently constituted SBN and is a small 'not for profit' organisation' and is exempt from notification. However it is still necessary to comply with the Data Protection Act and the eight principles.

Organisations that process personal data usually have to notify the Information Commissioner about this. Failure to notify is a criminal offence but some organisations are exempt. The website of the information commissioner has a guide to help decide whether or not there is a need to register with (notify) the Information Commissioner. http://www.ico.gov.uk/for_organisations/data_protection/notification/need_to_notify.aspx

Charities and voluntary groups which are 'not for profit' are still able to make a profit for their own purposes, which are usually charitable or social, but the profit should not be used to enrich others. Any money that is raised should be used for the organisation's own activities

In order to be exempt data/information processing must only be for the purposes of:

- establishing or maintaining membership;
- supporting a not-for-profit body or association; or
- providing or administering activities for either the members or those who have regular contact with it.

This would include giving support to individuals. It is also clear that although the contact the organisation has with people should be regular, it does not need to be frequent. So an organisation that provides activities or support on an ongoing basis to the same individuals (even if a minority only contact the organisation once) will fall within the exemption. However, one that deals with either few or many individuals on a one-off or isolated basis, such as in a drop-in centre, will not.

The exemption also restricts:
- the type of personal information an organisation can hold;
- the people that it relates to; and
- the disclosures that an organisation can make;

to only those necessary for the purposes described above unless the individual agrees their personal information can be released. The information must not be kept after the relationship between the individual and the organisation ends, unless it is necessary for the purposes described above.

Dealing with confidential/sensitive information or information about employees

It is unlikely that SBN will be collecting confidential or sensitive personal information or that it will have any direct employees. If that were to change in future then there would be a need to put in place procedures to deal with the new situation

Dealing with a data protection request

Under data protection law, anyone can ask if SBN holds personal information about them - we must respond to their request within 40 days. We can charge them up to £10 to provide the information. Again we may think that SBN is unlikely to fall into this category but see point (ii) below

As this sort of request is often made by individuals when they are in a dispute with the organisation it is important to bear in mind when data is collected or recorded that it may be questioned in the future.

The person has the right to know:

- what information is being used
- why it's being used
- where it came from
- who can see the information

They would have to be sent a hard copy, if possible - like a letter or print out - unless both agree otherwise. If you ignore the request or don't provide the information, you could be given a heavy fine by the Information Commissioner's Office.

The Information Commissioner has recently given advice on what type of personal data must be disclosed if an organisation receives a data access request. (See www.ico.gov.uk) The key steps which must be followed when deciding whether to disclose personal data are that data should be disclosed if:

(i) a living individual can be identified from the data;
(ii) the data relates to the identifiable living individual, whether in personal or family life, **business or profession;**
(iii) that data is obviously about a particular individual;
(iv) the data linked to the individual provides particular information about that individual;
(v) the data is used to inform or influence actions or decisions affecting an identifiable individual;
(vi) the data had biographical significance in relation to the individual;
(vii) the data focuses or concentrates on the individual as its central theme rather than some other person; or
(viii) the data impacts or has the potential to impact on an individual whether in a person, family, business or professional capacity.

Particular care must be taken when disclosing information if a third party can be identified from the data. Special provisions apply in such circumstances.

Chris Hounsell

04/01/13