

**POLICY NUMBER 18  
DATA PROTECTION POLICY  
HATCH WARREN & BEGGARWOOD COMMUNITY ASSOCIATION**

### Introduction

The Data Protection Act 1998 (The Act) requires organisations to ensure appropriate security measures exist for all data held. This is in order to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage.

The Act applies to organisations holding information about living individuals in electronic format and on paper. This includes information such as name, address, date of birth and opinions about the individual or any other information from which the individual can be identified.

All processing of data regarding personal information is covered by the Act, that is to say, the obtaining, disclosing, recording, holding, using, erasing or destroying of information.

Organisations must follow the eight data protection principles of good information handling. These say that personal information must be:

- fairly and lawfully processed
- processed for specified purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than necessary
- processed in line with the rights of the individual
- kept secure
- not transferred outside of the European Economic Area unless adequately protected

A register is held (by the Information Commissioner) which records organisations that control data and the purposes for which they use it. Registration (notification) is mandatory for all those holding data and re-registration is necessary on an annual basis.

### Policy definition

This policy defines our standards for the protection of data held and our rulings within the pertinent day-to-day handling areas.

If you have any queries regarding this policy please refer in the first instance to the data protection officer.

### Index

Please find below a list of the topics within this policy.

- Personal information
  - ↳ Control
  - ↳ Data security
  - ↳ Fair use of personal information
  - ↳ Data type
- Obligations and Rights
  - ↳ Employer obligations
  - ↳ Marketing
  - ↳ Electronic mail
  - ↳ Outsourcing

- ↳ Employee obligations
- ↳ Rights of individuals whose data we hold
- Requests for information
  - ↳ Handling requests
  - ↳ Releasing information to third parties
  - ↳ Releasing information in order to detect crime
- Breaching the data protection rules
- Addendum – General Data Protection Regulations (GDPR) – extension 2018

## Personal information

### ↳ **Control**

A company, as the legal entity, is responsible for overall compliance with the Data Protection Act. However the Acts' requirements also extend to staff obligations.

It is important that we define the different levels of data that we hold. We deal with businesses and individuals, we also deal with our own staff's personal data. We are responsible for all data we hold, whoever it is for and thus the same protections should be extended over all dealings we have. The person or business whom we hold data for is known as the 'data subject'. It is necessary that we ensure that any and all personal data is handled and managed in strict accordance with the requirements in this policy. By personal data we mean data we are holding regarding an individual. Data regarding businesses, for example their name, address etc, is not subject to this legislation.

We must make sure that we all understand and are clear about what we can and cannot do with the personal information we use, including to whom it can and cannot be disclosed. This extends to media attention and press releases and also to the protection/retention of information should a staff member leave.

### ↳ **Data security**

We should;

- keep passwords secure and change them regularly (system has an auto change request built in)
- lock or log off computers when away from the desk
- dispose of confidential paper waste securely by shredding or pulping
- prevent virus attacks by taking care when opening emails and attachments or visiting new websites
- work on a 'clear desk' basis (as near as possible)
- securely store hard copy information when it is not being used
- ensure visitors sign in and out of the premises and are accompanied in staff restricted areas
- encrypt if possible or take extra care with personal information that is being taken out of the office
- keep back-ups of information

### ↳ **Fair use of personal information**

It is important that data subjects understand what will happen to their personal information. We should therefore tell them;

- who is responsible for handling their personal information, and
- what their personal information will be used for.

(we should tell individuals about any disclosures we make, unless it is obvious. We should also tell them whether any credit searches will take place and what the consequences of those could be – footprint etc.)

We should also be careful not to use personal information we hold in a way that is outside what our clients would reasonably expect.

#### ↳ **Data type**

There are two types of data, personal and sensitive.

To hold personal data we do not require any specific permissions, the handing over of the information by the individual is the 'implied' permission for us to hold it.

We do however require specific permission to hold information that is regarded as sensitive. We will require explicit permission from the individual. This is normally a permission granted in writing or by another method of positive agreement, for example, signature.

- Personal data is anything which will identify an individual. This is mainly their name, address and date of birth.

- Sensitive personal data will include such areas as;

racial or ethnic origin

physical or mental health and condition

religious beliefs

sexual life

political opinion

any offences, alleged offences or proceedings for offences

### **Obligations and Rights**

#### ↳ **Employer obligations**

The employer must;

- register the holding of data with the Information Commissioner and maintain these records

- nominate one person within the organisation to be responsible for data protection

- notify their staff who the data protection officer is and provide contact details for this person

- follow the eight data protection principles and ensure that their staff also do

- initially train their staff (and then re-train/refresh regularly)

- audit the internal data protection policy and procedures on an annual basis

- deal with breach occurrences as appropriate and notify of breaches formally where necessary

- ensure information is destroyed appropriately, on a timely basis and securely (shredding/pulping)

- not intrude on anyone's right to privacy

- ensure that access to personal information is limited to those with a strict need to know

#### ↳ **Marketing**

Should we wish to promote our business and the products and services we sell, we should tell individuals at the outset and give them the opportunity to object. If an individual does object, either initially or later, we must not send that individual direct marketing again unless the individual specifically asks for it.

#### ↳ **Electronic mail (Email)**

We can only carry out unsolicited marketing (that is, marketing which has not specifically been asked for) by electronic mail if the individual we are sending the message to has given permission.

There is an exception to this rule, which is known as the 'soft opt-in', which applies where:

- we have obtained the individual's details in the course of a sale of a product or service

- the messages are only marketing our similar products or services

- the individual is given a simple opportunity to refuse the marketing when their details are collected

- the individual is given a simple way to opt out on a regular basis

We have to provide a valid address so that the individual can contact us if they want to stop the marketing and we must comply with any opt-out requests promptly.

### **Businesses and emails:**

The rules on email do not apply to emails sent to organisations except that we must still identify ourselves and provide an address.

However, that said, many individuals will provide their personal corporate email addresses and individual employees have a personal right under the Act to require us to stop using their address for marketing. Therefore, the personal rules above will apply.

#### ↳ Outsourcing

When organisations contract or arrange with someone to process personal information on their behalf they remain responsible for the processing. This means that we will remain liable for breaches of the Act. By way of example, this will include our agreements and work with archiving firms, solicitors, accountants, stationers, document disposal businesses and IT firms to name a few.

External companies we choose to use therefore, should be ones we consider can carry out work for us in a secure manner. We should also have a written contract in place with them; the contract must make sure that they only use and disclose data in line with our instructions and security measures.

#### ↳ Employee obligations

The employee must;

- follow the eight data protection principles
- concur and follow the data protection training and company standards, rules and requirements
- notify their data protection officer where it is believed a requirement has been breached
- not intrude on anyone's right to privacy

#### ↳ Rights of individuals whose data we hold

The Act gives individuals certain rights and we need to be aware of these rights.

- access to their information (please see handling requests below)
- prevent unsolicited marketing; allows them to request not to receive direct marketing
- prevent automated decision making; allows them to object to automatic (non-human) decisions
- claiming compensation; allows them to claim compensation for damage (and in some cases distress) caused by a breach of the Act
- correcting information; allows them to request their details are changed where there are inaccuracies
- prevent processing of their information; allows them to ask for information not to be processed where it may cause significant damage or distress. (We are not bound to act however)
- investigation; allows them to ask the Information Commissioner to investigate and assess whether an organisation (holding their data) has breached the Act.

### Requests for information

#### ↳ Handling requests

Disclosing customer personal information over the telephone;

We must carry out two identity checks before giving out personal information to someone making an incoming call. For example; name check and any personal information only the individual would know.

Handling requests from individuals for a hard copy (paper copy) of their personal information;

We have a maximum of 30 days to respond to any reasonable request and the maximum fee that can be charged is £10.00. We should always check the requester's identity. Before the information is sent out, we should check through it to ensure that we are not releasing anyone else's information. If another person's information is contained in the proposed response it must be blanked out.

↳ Releasing information to third parties

This is only to be completed if written authority has been provided by the individual whom the data is regarding. We should always check the requester's identity.

↳ **Releasing information in order to detect crime**

There is an exemption in the Data Protection Act 1998 that allows us to give out personal information in order to detect crime but there are limits on what can be released.

The police are most likely to use this exemption. However, other organisations who have a crime prevention or law enforcement function, for example, the Department for Work and Pensions – Benefit Fraud Section can also use this exemption.

The exemption does not cover the disclosure of all personal information, in all circumstances. It only allows us to release personal information for the stated purposes and, only, if not releasing it would be likely to significantly harm any attempt to prevent crime or catch a suspect.

For every request for personal information received (and about each separate individual), we need to be confident that;

- the person is who they say they are
- the person asking for this information is doing so to prevent/detect a crime or catch/prosecute an offender
- if the information is not released it will significantly harm any attempt by the police to prevent crime or catch a suspect

### **Breaching the data protection rules**

A data security breach can happen for a number of reasons:

- loss or theft of data or equipment on which data is stored
- inappropriate access controls allowing unauthorised use
- human error
- unforeseen circumstances such as a fire or flood
- hacking attack
- information obtained by deceit

If you believe a breach has occurred, please notify the data protection officer immediately.

### **Addendum – General Data Protection Regulations (GDPR) extension 2018**

The Data Protection Act 1998 (the "DPA"), the cornerstone of UK data protection law will be enhanced to include and incorporate the General Data Protection Regulations (GDPR), passed by the European Parliament

in April 2016. Enforcement of this is expected to be May 2018. This regulation is directly applicable to all member states of the EU, however given the Brexit results, it will still apply to the UK, as it is likely that European firms will not deal with countries that do not have parity of legislation.

Key Changes:

- Higher fines – fines up to 4% of a company's worldwide turnover or €20,000,000 (whichever is higher) can be imposed following a breach of the GDPR. The current maximum is £500,000. So this is a significant increase.
- Mandatory notification – it will be mandatory to report all breaches of data protection to the Information Commissioner without undue delay and within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk for the rights and freedoms of individuals. Currently, this procedure is voluntary.
- Sensitive personal data – stricter rules apply to processing of sensitive personal data such as medical information. What constitutes sensitive personal data has also been widened and will now include genetic and biometric data (e.g. retinal scans and fingerprints).
- Consent – obtaining consent will be harder. Silence or inactivity will not constitute consent. Consent must be freely given, specific, informed and unambiguous, provided by clear affirmative statement or action and which is able to be easily withdrawn. Businesses should not acquire consent by forcing a user to consent to one form of processing which is not necessary to the service the user is looking to receive. Parents will be required to provide their consent to the processing of children's personal data where those children are under a particular age (varying between 13 to 16 years old).
- Additional rights for data subjects - there will be a new right to transfer your data from one service provider to the other. Data requests are reducing from 40 days to 30, so firms need to be aware that they have less time to comply (to provide the data required).
- Mandatory Data Protection Officers – data controllers and processors whose core activities consist of processing sensitive personal data and / or regularly and systematically monitoring data subjects on a large scale (including monitoring consumer behaviour) and public authorities (other than courts acting in a judicial capacity) must appoint a data protection officer. A data protection officer's role will be to deal with data protection issues for the organisation.
- Data Processors - The DPA currently only regulates data controllers. The GDPR seeks to impose direct obligations on data processors as well as data controllers too. For example, data processors will be required to notify data controllers where there has been a breach and to obtain consent from a data controller before using any sub-processors. More detailed data controller to data processor contracts will be required as a result.

This policy was signed and approved at a meeting of the Hatch Warren & Beggarwood Community Association on:

Date: 26-6-2019

Signed:  (Chairperson)