

Kingston Churches Housing Association

The Caring Professionals

DATA PROTECTION ACT 2018 POLICY AND PROCEDURE

INTRODUCTION

Personal data about living individuals is protected by the Data Protection Act 2018 (the DPA). The Act came into force on 25th May 2018, replacing earlier 1998 legislation to sit alongside the General Data Protection Regulation (GDPR) and tailoring the GDPR for implementation in Britain. Those processing personal data have to follow six data protection principles. They also have to comply with other provisions of the Act such as giving individuals rights of access to their data.

The DPA aims to promote high standards in the handling of personal information and so to protect the individual's right to privacy. It establishes a framework of rights and duties designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business purposes against the right of individuals to respect for the privacy of their personal data. Although the legislation is complex, it is underpinned by a set of six straightforward, common-sense principles. The new act is designed for a new digital age and to ensure that UK and EU data protecting regimes are aligned pre and post Brexit.

REGISTRATION

The DPA requires the Information Commissioner to maintain a Register of certain data controllers (broadly speaking, firms and others who are responsible for processing information) and the purposes for which they use personal information.

The Association is a registered data controller under the Act.

TYPES OF DATA

Personal data

The Act applies to personal data. This is information about living individuals. It would include a person's name and address or email address. It would cover photographs of people, but would not include company names and addresses. It applies to data on computers and also manual data in a relevant filing system where

it is part of a structured set. It also applies to online digital services such as social media and our website for which a privacy notice is clearly declared.

Sensitive personal data

Section 2 of the Act defines sensitive personal data as information relating to:

- (a) Racial or ethnic origin of the data subject
- (b) Political opinions
- (c) Religious beliefs or beliefs of a similar nature
- (d) Membership of a trade union or non-membership
- (e) Physical or mental health or condition
- (f) Sexual life
- (g) The commission or alleged commission of any offence, or
- (h) Any proceedings for an offence committed or alleged to have been committed by him or her, the disposal of any such proceedings or the sentence of any court to such proceedings.

7 DATA PROTECTION PRINCIPLES - GDPR (Article 5)

Processing personal data

'Processing' is broadly defined and takes place when any operation or set of operations is carried out on personal data. The DPA's *principle (a)* requires that personal data must be processed with "lawfulness, fairness and transparency". Personal data will not be considered to be processed fairly unless certain conditions (given in Schedule 2) are met. A data subject must be told the identity of the data controller and why the information is to be processed.

Processing may only be carried out where one of the following conditions has been met:

- (a) The individual has given his or her explicit consent to the processing.
- (b) The processing is necessary for the performance of a contract with the individual.
- (c) The processing is required under a legal obligation.
- (d) The processing is necessary to protect the vital interests of the individual.
- (e) The processing is necessary to carry out public functions.
- (f) The processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interest of the individual).

Processing sensitive data

The DPA makes specific provision for sensitive personal data as defined above. This can only be processed under strict conditions (given in Schedule 3), which include:

- (a) Having the explicit consent of the individual.
- (b) Being required by law to process the data for employment purposes.
- (c) Needing to process the information in order to protect the vital interests of the data subject or another.
- (d) Dealing with the administration of justice or legal proceedings.

Data obtained only for stated purpose

The DPA's *principle (b)* requires that personal data should be "obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

Data adequate, relevant and not excessive

Principle (c) says that personal data must be adequate, relevant and not excessive in relation to the purposes for which it is processed.

Data accurate and up to date

Principle (d) provides that data shall be accurate and where necessary kept up to date.

Data not retained longer than necessary

Principle (e) states that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Data to be processed in accordance with the Act

Principle (f) states that data shall be processed in accordance with the rights of data subjects under the DPA to include appropriate security measures to protect against unauthorised processing, accidental loss, destruction and damage.

Principle (g) adds "The controller shall be responsible for, and be able to demonstrate compliance."

SUBJECT ACCESS REQUESTS

The DPA also gives individuals certain rights, including the right to see information that is held about them and to have it corrected if it is wrong. This right enables individuals to get a copy of information held on computer and in some manual filing systems, and is known as the right of subject access.

If anyone requests to see information, the position should be checked with the Information Commissioner's Officer (ICO) - see Helpline details below.

If a subject access request is received, it must be dealt with promptly and normally within 20 days of receipt. A fee may be charged in some cases for actual costs incurred. It is recognised that proportionality can be used sparingly when providing such information may be too resource intensive.

There are some circumstances where there is not a requirement to supply personal information or information about other people. **If in any doubt, advice should be sought from the ICO.**

FOR STAFF INFORMATION

Breaches

All breaches and potential breaches need to be reported to the most senior member of staff available. The details are then recorded on a register including any actions taken as a result of the breach. All significant breaches will need to be reported to the Information Commissioner's Officer at the earliest opportunity within a 72 hour deadline. **If in any doubt, the procedure requires you to contact the ICO immediately for advice.**

Consent

Wherever we require anyone to complete an application form or monitoring information we have now included in the form a statement on the Data Protection Act 2018 and we ask them to confirm their consent in accordance with the Act.

Listed below are the forms which have the DPA Statement added to them:

Approved Contractors/Consultants Application Pack
Sheltered Application Form
Housing Application Form
Job Application Pack
Self Certification of Sickness Form
Employment Reference Form
Employee Personnel File Details
Request for Exchange
Home Visit Form
Pets Request Form
Declaration of Interests
Board Members Application
Share Membership Form
Ethnic Monitoring

If you identify any other forms please let the Chief Executive know.

Document Retention

We should not keep information for longer than is necessary. Please refer to the National Housing Federation 2018 Document Retention and disposal Schedule which can be downloaded online at: <https://www.housing.org.uk/resource-library/browse/document-retention-and-disposal-for-housing-associations/>

The main implications for us are tenants and employee details.

Security

We should ensure that data is held securely and not available to tenants or other visitors, and that sources of data are locked at the end of each working day.

Information Commissioner's Office Helpline and Other Contact Details

Tel: 0303 123 1113. The helpline is open from 9am to 5pm, Monday to Friday.

Fax: 01625 524510

Email: dataprotectionfee@ico.org.uk / casework@ico.org.uk

Website: <https://ico.org.uk>

Address (head office)

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF