Quadrant - Brownswood Tenant Co-operative Ltd.

DATA PROTECTION AND CONFIDENTIALITY POLICY
Approved by MC: December 2018
Review date: November 2020

STATEMENT OF INTENT
The General Data Protection Regulation (GDPR) of 2016 came into effect from 25 May 2018 and, along with the Data Protection Act 2018, replaces the Data Protection Act 1998. Its purpose is to protect the 'rights and freedoms' of living individuals in relation to the use of their personal information and to ensure that personal data is not processed without their knowledge.

The term "Data Protection Legislation" is used in this policy to denote the collective Data Protection law (of GDPR and UK Act). All Data Protection Legislation in the UK is regulated by a supervisory authority called the Information Commissioner's Office (ICO).

QBTC is a data controller under Data Protection Legislation - for personal data processing and makes decisions about how and why it is processed.

OBJECTIVE OF THIS POLICY
This policy describes how the co-op intends to meet its legal responsibilities in respect of Data Protection legislation, and how we ensure that all members of the co-op know what their individual responsibilities are.

The policy's objectives are to:
- protect the personal data interests of individuals and other key stakeholders by the use of appropriate procedures and controls;
- provide the supporting framework for achieving and maintaining compliance;
- ensure the co-op meets applicable statutory, regulatory, contractual and/or professional duties

GUIDING PRINCIPLES
We are committed to ensuring that we comply with the six data protection principles and the other requirements of GDPR, as follows:
- Personal data must be processed lawfully, fairly and transparently
- Personal data can only be collected for specified, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to the purpose for which the data is processed
- Personal data must be accurate and kept up to date
- Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for the processing purposes
- Personal data must be processed in a manner that ensures the appropriate security.

And, in addition:
- To ensure that data protection is taken seriously and a key consideration of decisions we make
- To ensure that the data the co-op holds about individuals is properly managed
- Where legitimate, to make the personal data the co-op holds about individuals accessible

- To ensure that all co-op members are aware of their rights, responsibilities and liabilities in terms of data collection, holding, use and/or disclosure

WHAT IS PERSONAL DATA?

The co-op necessarily and routinely uses personal data information when it carries out many aspects of its day to day business. The organisation is subject to this policy, with some requirements spreading out and imposing responsibilities on partner organisations, e.g. our maintenance contractors, managing agent etc.

Personal data is all data within our computer systems, email, office files, plus manual structured filing systems that refers or relates to a living data subject (including those that are managed on our behalf by a managing agent, if applicable).

Special categories of personal data are considered more sensitive and need more protection. These include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

BREACH OF POLICY

A 'personal data breach' firstly involves a security incident which leads to compromise of data integrity, availability or confidentiality.

Any breach of Data Protection Legislation or this policy can be dealt with under the co-op's complaints policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Where a Co-op Officer, Management Committee member, or sub-committee member is responsible for a breach of a serious nature, the co-op will consider removing them from office.

DEFINITIONS

Breach of personal data: a breach of security leading to the accidental, or unlawful, destruction, loss, alteration,
unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the ICO, dependent on the seriousness, and whether the breach is likely to adversely affect the personal data or privacy of the data subject.

Data controller: a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

Data subject: any living individual who is the subject of personal data held by an organisation

Personal data: any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It covers information about living people stored on a computer or in an organised paper filing system, CCTV system, digital camera or audio recordings and digital images.

Third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

RESPONSIBILITIES

The Management Committee (or co-op officers if applicable) is ultimately responsible for compliance with relevant laws and is responsible for risk management. All members of the MC (and appropriate sub-committees) are expected to be familiar with this policy.

It is the responsibility of the MC and/or co-op officers to:

- Assess the understanding of the obligations of the co-op under the Data Protection legislation
- Be aware of the co-op's compliance status
- Identify and monitor problem areas and risks and recommend solutions; and
- Offer guidance to members on Data Protection issues
- Liaise with the ICO and individuals as appropriate
- Ensure that the co-op does not collect information that is not strictly necessary for the purpose for which it is obtained.

The co-op is responsible for ensuring that:

- they are aware of the provisions of the Act and its impact on the work they undertake on behalf of the co-op.
- personal data they hold, whether in electronic or paper format, is kept securely.
- personal data is not disclosed deliberately or accidentally either orally or in writing to any unauthorised 3rd party.

These responsibilities can be shared with the managing agent as appropriate.

ACCOUNTABILITY

The new Data Protection legislation introduces the principle of accountability which states that the Data Controller is not only responsible for ensuring compliance but also for demonstrating that each processing operation complies with Data Protection legislation. Specifically, Data Controllers are required to evidence compliance with the Regulation, which includes:

- maintaining necessary documentation of all processing operations;
- implementing appropriate security measures;
- carrying out Data Processing Impact Assessments (DPIAs);
- complying with requirements for prior notifications, or approval from supervisory authorities;
- appointing a DPO, if required.

LAWFUL BASIS FOR PROCESSING PERSONAL DATA

Personal data

The co-op will only collect and process personal data if one of the conditions set out below has been satisfied:

- the express consent of the tenant or employee (if applicable) is obtained prior to the processing of personal data. Consent must be freely given; it must also be specific and informed.
- processing is necessary for the performance of a contract to which the tenant or employee is party or in order to take steps at the request of the tenant or employee prior to entering into the contract;
- processing is necessary for compliance with a legal obligation to which the co-op is subject;
- processing is necessary in order to protect the vital interests of the tenant or employee or of another natural person;
- processing is necessary for performing a task in the public interest;

- processing is necessary for the purposes of the legitimate interests pursued by the co-op or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the tenant or employee which require protection of personal data, where the data subject is a child.

Special Categories of Personal Data
The co-op will only collect and process special categories of personal data if one of the conditions set out below has
also been satisfied:

- the data subject has freely given explicit consent to the processing of their personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment law and the controller has an appropriate policy document in place;
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;
- processing relates to personal data which has been made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest.;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, including the need to complete statutory or regulatory returns.

Lawful bases
The co-op will usually use three different lawful bases dependent on the circumstances:

- We process personal data 'for the purposes of legitimate interests' of providing and maintaining our properties (e.g. providing former-tenant references)
- Where we have a contract with the data subjects, we process personal data in order to fulfil it (e.g. tenancy agreement).
- We have a legal obligation to collect or use certain information (e.g. managing complaints)

The co-op is registered with the ICO as a data controller and has identified all the personal data that it processes. This is contained in the Processing Activity Record (PAR). A copy of the ICO registration is retained and renewed annually by the co-op (or through the managing agent).

DISCLOSURE OF DATA
We sometimes receive requests to disclose information to authorities in certain circumstances, for example, a request for information to:

- prevent or detect crime, including the apprehension and prosecution of offenders;
- assessing or collecting any tax or duty owed;
- preventing serious harm to a third party, including protecting the vital interests of the individual, e.g. in emergency medical situations

All requests to provide data for one of these reasons must be supported by appropriate

documentation to justify the decision and all such disclosures must be specifically authorised by the co-op. We will carefully balance a common sense approach with the requirements of the Data Protection Legislation. The following types of verification and limitation questions must be asked:

- Is the person requesting the information who they say they are?
- Is their intention to prevent or detect a crime, catch or prosecute an offender or assess or collect tax or duty?
- If the information is not released, will this significantly harm prevention of a crime or catching of a suspect? (The risk must be that the investigation may be impeded.)
- What is the minimum amount of information to enable them to do their job?
- What else needs to be known to be sure that we can disclose the information?

Information Sharing

The co-op must ensure that personal data is not disclosed to unauthorised third parties. This includes family members, friends and government bodies. All members should exercise caution when asked to disclose personal data held on an individual to a third-party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of co-op business.

There are a number of Information Sharing Agreements in place, e.g. with the police, councils and other agencies using set sharing protocols and which govern how and when to share information appropriately.

Management Committee members and co-op officers do not have any right to see personal data stored on files except as is necessary in the course of their duties. The same applies to any co-op officers and subcommittee members.

In certain limited circumstances Data Protection Legislation provides for personal data, even sensitive data, to be shared without the individual knowing about it.

Suppliers and Contractors

The co-op employs various contractors to carry out tasks and services on its behalf; some have a genuine need to use
personal data of our customers. Such contractors are known as data processors. These contractors are required to sign the information sharing protocol as part of the approved contractor list procedure. This sets out the standards and obligations that the co-op expects in the processing of personal data.

Data Protection Impact Assessment

There may be risks associated with the processing of particular types of personal data and particular circumstances, which the co-op must assess by means of a Data Protection Impact Assessment (DPIA). A DPIA can cover in-house processing of personal data and that undertaken by other organisations on behalf of the co-op. See the Data Protection Impact Assessment procedure (attached as **appendix 1**).

Where, as a result of a DPIA it is clear that the co-op is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not the co-op may proceed must be reviewed by the Management Committee or general members. If there are significant concerns that cannot be mitigated, the matter should be escalated to the ICO.

RECORDS AND HOUSEKEEPING

The co-op shall not keep personal data in a form that permits identification of data subjects for longer than is deemed necessary (in relation to the purpose(s) for which the data was originally collected).

The co-op follows the National Housing Federation document retention schedule for housing associations (latest version here: https://www.housing.org.uk/resource-library/browse/document-retention-and-disposal-for-housing- associations/). The retention periods should be used as a guide to understand when certain documents might no longer be needed. The key areas of the schedule are:

Records	Recommended retention period	Reason for retention
Board and committee	Permanently	Legal compliance
Applications for accommodation	6 years after offer accepted	Best practice
Application forms of non-short listed candidates	1 year	Legal compliance
Application short lists, interview notes and	1 year	Best practice
Rent statements	2 years	Best practice
Current tenants' Tenancy Files (including agreement, rent payment history, details of complaints, ASB, etc)	6 years (NB – QBTC has requested that this be kept for duration of tenancy)	Legal compliance
Former tenants' Tenancy Agreements & details of their leaving	6 years	Legal compliance
CCTV	30 days	DPA

VISUAL DATA (CCTV AND SURVEILLANCE)

The Co-op recognises its responsibility to provide its residents a safe and peaceful environment in which to live.

Where it proves necessary to support this, the co-op will introduce and maintain CCTV with guidance taken from The Information Commissioner's Office (ICO) code of practice under the General Data Protection Regulation (GDPR) 2018 and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (POFA code).

The Co-op's objective of installing CCTV and Surveillance Systems is:

- To prevent and detect crime, nuisance and antisocial behaviour.
- To improve the safety and security of the co-op's members and their visitors.
- To support the identification, apprehension and prosecution of offenders in both criminal and civil investigations.

The Co-op therefore aims to ensure that:

- CCTV is used effectively and for a specified purpose which is in pursuit of a legitimate aim, i.e. for public safety and law enforcement. For the co-op this is likely to apply to preventing anti-social behaviour and crime in and around the co-op's properties, alleged breaches of tenancy, and to help create a safer environment for its members;
- take into account its effect on individuals and their privacy and ensure there is as much transparency and accountability in the use of CCTV, including images and information collected as possible;
- access to images and information is restricted to safeguard against unauthorised access;
- disclosure to third parties will only take place for law enforcement where any images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness ; or, for subject access request purposes unless disclosure could prejudice the prevention or detection of crime or the apprehension or prosecution of an offender. Where the co-op is unable to comply with the request because access

could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, the persons involved will be advised accordingly;
- images will only be stored for the stated purpose and deleted once those purposes have been discharged;
- where cameras are installed signage will be displayed so that customers and any visitors to the locality are aware that CCTV is in operation;
- it is following best practice and acting within the law.

The Chair of the Management Committee, or another member acting on their authority, is permitted to authorise disclosure of information to external third parties such as law enforcement agencies. All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied the reason will be recorded.
Subject access requests will also be subject to this policy. The request must include the date and time the images were recorded and the location of the CCTV camera, so that the images can be located, identity can be established as the person in the images and the identity of any other person in the image anonymised.

SUBJECT ACCESS REQUESTS
The co-op will ensure that requests made by data subjects to access their personal data are responded to in accordance with the Act which requires that the data subject is provided with access to their personal data promptly and within 1 calendar month of their request being validated.

The co-op (via management committee or managing agent as applicable) needs to co-ordinate all subject access requests and ensure that all manual data in relevant filing systems are reviewed and any personal data relating to 3rd parties either redacted, anonymised or consent for its disclosure obtained from the 3rd party. This may be lead by an officer of the management committee (e.g. Secretary).

Personal data will only be disclosed to the data subject when:
- the subject access request is made in writing;
- the authenticity of the individual making the request has been confirmed.

Data collection involves:
- Searching all databases and all relevant filing systems (structured manual files), including all back up and archived files (computerised or manual), CCTV, and all email folders and archives. Collecting and extracting the data specified by the data subject;
- Personal data may be held in sources that are not immediately obvious. These must all be identified and searched. The responsible member reviews all data that has been collected to identify whether any third- party data are present in it, or whether any other exemptions apply that would stop us from providing the information.

There are a number of circumstances where there may be a legitimate reason for not complying with a SAR. These exemptions include the following:
- National security;
- Crime and taxation;
- Health;
- Education;
- Social work;
- Regulatory activity;

- Research history, and statistics;
- Publicly available information;
- Corporate finance;
- Confidential references;
- Management forecasts;
- Legal advice and proceedings
- Active negotiations with the data subject

Guidance on SAR process and exceptions should be sought from the ICO.

MEASURE OF SUCCESS

- Adherence to the Data Protection Act.
- Lawful and correct processing of personal data.
- Regular review by the QBTC management committee.
- Signed declaration of confidentiality (**appendix 2**) for all members of the management committee, co-op officers, and subcommittee members (as applicable).

Appendix 1 - Data Protection Impact Assessment

Is a DPIA necessary?
It's sensible to firstly establish whether a DPIA is necessary in a new or changed situation to determine if the proposed type of processing, its' nature, scope, context or purpose is likely to result in a high risk to the 'rights and freedoms' of individuals. The DPIA must be carried out prior to the processing and a single assessment may address a set of similar processing operations that present similar high risks.

Examples of projects which may require a DPIA include:

- A new IT system for storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data

Screening questions

1. Will the project involve the collection of new information about individuals?
2. Will the project require individuals to provide information about themselves?
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
4. Is information about individuals being used for a purpose or in a way it's not currently being used?
5. Does the project involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
6. Will the project result in making decisions or taking action against individuals in ways which can have a significant impact on them?
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations, for example, health records, criminal records or other information that people would consider to be particularly private?
8. Will the project require the contacting of individuals in ways which they may find intrusive?

There is no fixed template for completing a DPIA. Please refer to the ICO's suggested DPIA template found here https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact- assessments-dpias/what-is-a-dpia/

DPIAs are designed to be a flexible and scalable tool which can be integrated with the co-op's existing approach to managing projects. Conducting a DPIA doesn't have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising.

A DPIA should begin early in the life of a project but can run alongside the project development process.

Appendix 2 – declaration of confidentiality

The Management Committee (and subcommittees as applicable) meets regularly in order to complete the day to day running of co-op business. It is absolutely essential that any and all information that pertains to the co-op remains private and confidential. It is against the Data Protection Act to take, use or misuse information that could be in any way be construed as belonging to the co-op or it's members. This also means that such information should not be passed on, discussed or even alluded to outside of a convened meeting, as the future wellbeing of the co-op could be affected.

Confidential information must not be used for personal gain, and all data which is not in the public domain is deemed to be confidential. This includes information relating to the co-op and to other parties who have dealings with the co- op. To this end, all members of all Committees and co-op officers should sign a declaration stating their agreement not to divulge any aforementioned information, as detailed above. Members joining Committees will be asked to sign a declaration prior to taking their place within the group.

I hereby declare that I will not, at any time, divulge any such information pertaining to

the co-op or its members. Should I know of anyone who passes on such information I will

immediately inform the Management Committee (or
managing agent as applicable).

I understand that if I am found to have divulged such information I may be subject to action which could ultimately result in my tenancy being revoked.

Name:……..

Signature……

Date:……

Position:……