Cloch Housing Association

Appropriate Document Policy

Policy Name	Appropriate Document Policy
Policy Category	Corporate & Governance
Policy Number	112
Approved by	Board or F&CS Sub-Committee
Responsibility of	Corporate Services
Date Adopted	02/06/2022
Last Review	02/06/2022
This Review	03/09/2024
Next Review	September 2027
Equalities Impact Assessment Required	No
Link to other policies	Privacy Notice, Data Protection Policy
Consultation	No
Need for Procedure	No

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require you to have an APD in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document should demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular, it should outline your retention policies with respect to this data. (See Schedule 1 Part 4).

If you process SC or CO data for a number of different purposes you do not need a separate policy document for each condition or processing activity – one document can cover them all. You may reference policies and procedures which are relevant to all the identified processing. Whilst you may explain your compliance with the principles in general terms, without specific reference to each individual Schedule 1 condition you have listed, you should provide the data subject with sufficient information to understand how you are processing their SC or CO data and how long you will retain it for.

However if you rely on one of these conditions, your general record of processing activities under GDPR Article 30 must include:

(a) the condition which is relied upon;
(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and
(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

The APD therefore complements your general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. See Schedule 1 Part 4 paragraph 41.

You must keep the APD under review and will need to retain it until six months after the date you stop the relevant processing. If the Commissioner asks to see it, you must provide it free of charge. See Schedule 1 Part 4 paragraph 40.

You should read this document alongside the ICO Guide to the GDPR.
Note your APD does not have to be structured in accordance with this document. This template is intended as a guideline only.

Description of data processed

Give a brief description of each category of SC/CO data processed. You may wish to refer to your Article 30 record of processing for that particular data:

Corporate Services

- Members – disability details, ethnic origin
- Prospective employees – recruitment applications including health data, ethnicity, disability, gender, criminal convictions
- Current employees – contract of employment management, declarations of interest, disclosure information, employee wellbeing including personal health information, medication, allergies, trade union membership if the employee pays through their salary, religion and belief (potentially), criminal convictions/cautions (if relevant), biometric data

Health and Safety

- Tenants, employees, residents, visitors, members of the public and contractors – H&S legislation compliance including health data

Property and Housing

- Current, prospective and former customers and tenants - ASB/Confidential information from Police Scotland and info about sex offenders
- Current, prospective and former customers and tenants - Disabilities/Medical info
- Current, prospective and former tenants - Ethnic Origin – currently we have this on a tenant file. Soon to be anonymised.

IT

- Employees, contractors, suppliers, residents, tenants – any stored special category data

Schedule 1 condition for processing

Give the name and paragraph number of your relevant Schedule 1 condition(s) for processing. Alternatively, you may wish to provide a link to your privacy policy, your record of processing or any other relevant documentation:

As per ROPA

- Employment – 1
- Health or social care purposes – 2
- Public Health - 3
- Equality - 8
- Racial and ethnic diversity – 9
- Consent (Art 9)

Procedures for ensuring compliance with the principles

You need to explain, in brief and with reference to the conditions relied upon, how your procedures ensure your compliance with the principles below.

This helps you meet your accountability obligations. You have a responsibility to demonstrate that your policies and procedures ensure your compliance with the wider requirements of the GDPR and in particular the principles. The sensitivity of SC and CO data means the technical and organisational measures you have in place to protect such data are crucially important.

The questions listed in each box are intended to help you describe how you satisfy each principle generally, and are based on the checklist for each principle provided in the Guide to the GDPR. They are not exhaustive and are only intended to act as a guideline.

In explaining your compliance with the principles you should consider the specifics of your processing with respect to the SC and CO data you have identified above.
You may also wish to answer other questions which are included in our Guide to the GDPR checklists (see links in each section below).

There is also no requirement to reproduce information which is recorded elsewhere – **questions may be answered with a link or reference to other documentation, to your policies and procedures, Data Protection Impact Assessments (DPIAs) or to your privacy notices.**

Accountability principle
i. Do we maintain appropriate documentation of our processing activities? ii. Do we have appropriate data protection policies? iii. Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests? See general checklist for Accountability and Governance. Yes i. we have an Art 30 ROPA ii. We also have policies for privacy, breach management, data protection policy and subject access request policy iii. We have a DPIA procedure and various other procedures which support the lawfulness of processing activities.
Principle (a): lawfulness, fairness and transparency
i. Have we identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data? ii. Do we make appropriate privacy information available with respect to the SC/CO data? iii. Are we open and honest when we collect the SC/CO data and do we ensure we do not deceive or mislead people about its use? See general checklist for Lawfulness, fairness and transparency. Yes i. Recorded on our RoPA ii. Through our privacy notices iii. Through our privacy notices
Principle (b): purpose limitation
i. Have we clearly identified our purpose(s) for processing the SC/CO data? ii. Have we included appropriate details of these purposes in our privacy information for individuals? iii. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?

See general checklist for purpose limitation.

Please see our Register of Processing, Privacy Notice, Fair Processing Notice and our Data Impact Assessments.

Yes

i. Recorded on our RoPA
ii. See Website Data Protection statement and privacy notices
iii. Yes

Principle (c): data minimisation

i. Are we satisfied that we only collect SC/CO personal data we actually need for our specified purposes?
ii. Are we satisfied that we have sufficient SC/CO data to properly fulfil those purposes?
iii. Do we periodically review this particular SC/CO data, and delete anything we don't need?

See general checklist for Data minimisation.

Yes, primarily demonstrated through our Retention Policy and Schedule.

i. Yes, as recorded on RoPA
ii. Yes
iii. Yes, as per Retention policy and schedule

Principle (d): accuracy

i. Do we have appropriate processes in place to check the accuracy of the SC/CO data we collect, and do we record the source of that data?
ii. Do we have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and do we update it as necessary?
iii. Do we have a policy or set of procedures which outline how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification?

See general checklist for Accuracy.

Yes

i. SC/CO data is obtained from Disclosure Scotland, all other SC/CO data is provided by the data subjects
ii. SC/CO data is updated where necessary
iii. Yes – as per Data Protection Policy and Subject Rights procedure

Principle (e): storage limitation

i. Do we carefully consider how long we keep the SC/CO data and can we justify this amount of time?
ii. Do we regularly review our information and erase or anonymise this SC/CO data when we no longer need it?
iii. Have we clearly identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes?

See general checklist for Storage limitation.

Yes.
i. primarily demonstrated through our Retention Policy and Schedule
ii. primarily demonstrated through our Retention Policy and Schedule
iii. none identified less for statistical reporting (to the Scottish Housing Regulator)

Principle (f): integrity and confidentiality (security)

i. Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?
ii. Do we have an information security policy (or equivalent) regarding this SC/CO data and do we take steps to make sure the policy is implemented? Is it regularly reviewed?
iii. Have we put other technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing?

See general checklist for Security.

i. Yes - Data Protection Compliance Audit first conducted 21 Novemeber 2018 and continues to be monitored through our ongoing GDPR action plan
ii. Yes – as per IT Security Strategy
iii. Email encryption service and Two-Factor authentication is in place for staff to access their emails. We are also Cyber Essentials certified.

Retention and erasure policies

You need to explain your retention and erasure policies with respect to each category of SC/CO data (this could include a link to your retention policy if you have one). You need to explicitly indicate how long you are likely to retain each specific category of SC/CO data.

We have retention levels in our register of processing.

Former employee data is erased after 6 years (or after 10 years if a compromise agreement has been signed)
Former customer data is erased after 6 years.
Confidential Finance information after 7 years.

Our retention policy and schedule is due for review in 2027.

APD review date

This policy will be reviewed annually or revised more frequently if necessary
Reviewed August 2024
Next review due August 2025