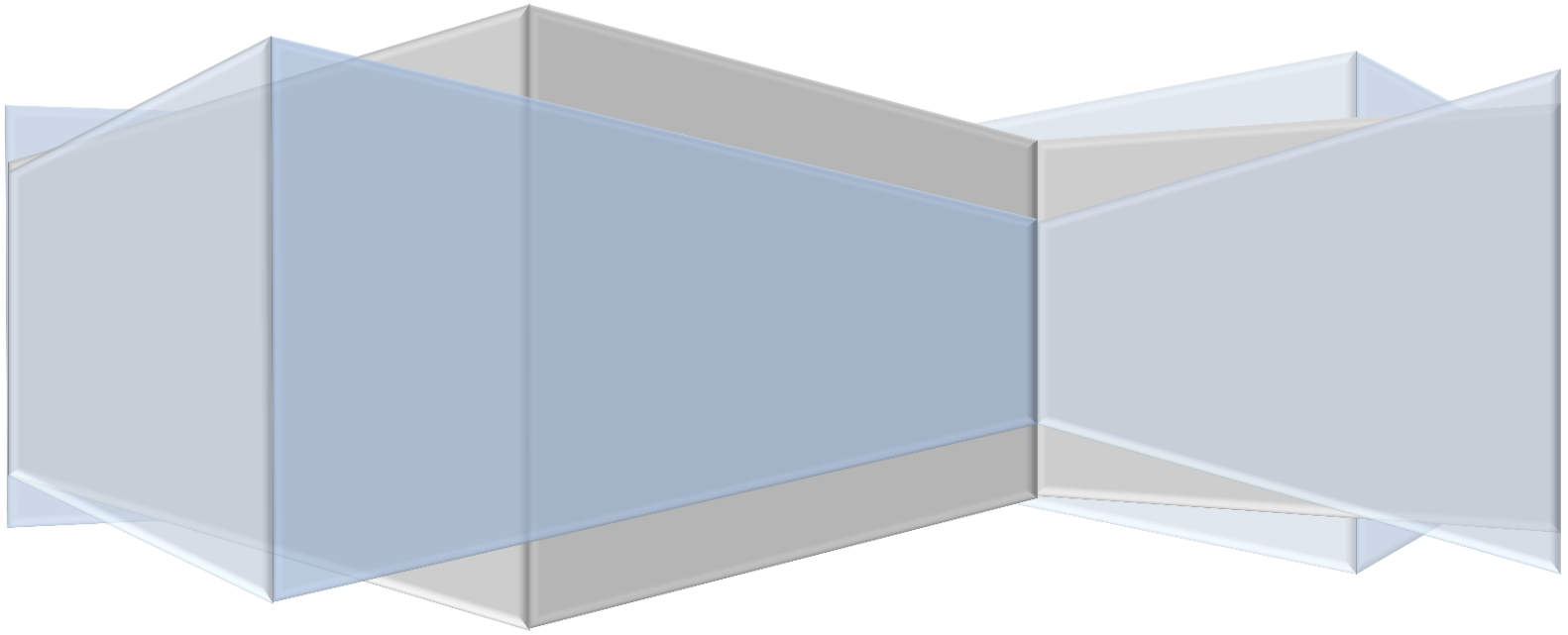
Data Protection Policy

November 2019



All Policies are available on tape, in braille and in translationin to most languages. Please ask a member of staff if you would like this policy in a different format

Date of Policy Review: November 2019
Date of Committee Approval: 3rd December 2019
Date of Next Review: November 2022

SCOTTISH HOUSING REGULATOR STANDARDS	STANDARD 1: The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users. STANDARD 2: The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. Its primary focus is the sustainable achievement of these priorities. STANDARD 4: The governing body bases its decisions on good quality information and advice, and identifies and mitigates risks to the organisation's purpose. STANDARD 5: The RSL conducts its affairs with honesty and integrity. STANDARD 6: The governing body and senior officers have the skills and knowledge they need to be effective.

Contents:

1. Introduction

Cathcart & District Housing Association (CDHA) is committed to ensuring the secure and safe management of data held by CDHA in relation to customers, staff and other individuals. CDHA's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

CDHA needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that CDHA has a relationship with. CDHA manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the General Data Protection Regulation (GDPR).

This Policy sets out CDHA's duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

2. Legislation

It is a legal requirement that CDHA process data correctly; CDHA must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

(a) the General Data Protection Regulation (EU) 2016/679 ("the GDPR");

(b) the Data Protection Act 2018 (which brings the GDPR into UK law);

(c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

(d) any other legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.

3. Data

3.1 CDHA holds a variety of Data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by CDHA is detailed within the Employee Fair Processing Notice and the general public Fair Processing Notice.

3.1.1 "Personal Data" is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by CDHA.

3.1.2 CDHA also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4. Processing of Personal Data

4.1 **Personal Data**

CDHA is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see clause 4.4 hereof);
- Processing is necessary for the performance of a contract between CDHA and the data subject or for entering into a contract with the data subject;
- Processing is necessary for CDHA's compliance with a legal obligation;

- Processing is necessary to protect the vital interests of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of CDHA's official authority; or
- Processing is necessary for the purposes of CDHA's legitimate interests or the legitimate interests of a third party, provided that such processing does not override the individual rights and freedoms of the data subject.

4.2 **Fair Processing Notice**

4.2.1 CDHA has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal Data is held by CDHA. That FPN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them.

4.2.2 The Fair Processing Notices set out the Personal Data processed by CDHA and the basis for that Processing. The general or public Fair Processing Notice is provided to all of CDHA's customers at the outset of processing their data, and the Employee Fair Processing Notice is provided to all employees at the outset of their employment.

4.3 **Employees**

Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by CDHA. Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to Employees at the same time as their Contract of Employment.

4.4 **Consent**

Consent as a ground of processing will require to be used from time to time by CDHA when processing Personal Data. It should be used by CDHA where no other alternative ground for processing is available. In the event that CDHA requires to obtain consent to process a data subject's

Personal Data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form, or take some other form of affirmative action, if willing to consent. Any consent to be obtained by CDHA must be for a specific and defined purpose (i.e. general consent cannot be sought).

4.5 **Processing of Special Category Personal Data or Sensitive Personal Data**

In the event that CDHA processes Special Category Personal Data or Sensitive Personal Data, CDHA must do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest.

It is worth noting that the UK Data Protection Act 2018 defines what should be considered to be a "substantial public interest" for the purposes of processing Special Category Personal Data or criminal conviction data. Most processing of Special Category Personal Data by CDHA will fall within scope of this "substantial public interest" ground.

5. Data Sharing

CDHA shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with CDHA's relevant policies and procedures. In order that CDHA can monitor compliance by these third parties with Data Protection laws, CDHA will require the third party organisations to enter in to an Agreement with CDHA governing the processing of data, security measures to be implemented and responsibility for breaches.

5.1 **Data Sharing**

5.2.1 Personal data is from time to time shared amongst CDHA and third parties who require to process personal data for their own separate purposes. Both CDHA and the third party will be processing that data in their individual capacities as data controllers.

5.2.2 Where CDHA shares in the processing of Personal Data with a third party organisation (e.g. sharing with other housing associations or sharing with other public bodies), it shall require the third party organisation to enter in to a Data Sharing Agreement with CDHA in accordance with the terms of the model Data Sharing Agreement.

5.2 **Data Processors**

A data processor is a third party entity that processes personal data on behalf of CDHA in the delivery of its services to CDHA (e.g. payroll, maintenance and repair works).

5.2.1 A data processor must comply with Data Protection laws. CDHA's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify CDHA if a data breach occurs.

5.2.2 If a data processor wishes to sub-contract their processing, prior written consent of CDHA must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

5.2.3 Where CDHA contracts with a third party to process personal data held by CDHA, it shall require the third party to enter in to a Data Protection Addendum with CDHA in accordance with the terms of the model Data Protection Addendum.

6. Data Storage and Security

All Personal Data held by CDHA must be stored securely, whether electronically or in paper format.

6.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no Personal Data is left where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee so as to ensure its destruction. If the Personal Data requires to be retained on a physical file then the

employee should ensure that it is affixed to the file which is then stored in accordance with CDHA's storage provisions.

6.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to CDHA's data processors or those with whom CDHA has entered in to a Data Sharing Agreement. If Personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be encrypted and stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers with appropriate access controls in place.

7. Breaches

7.1 Data Breach

A data breach can occur at any point when handling Personal Data and CDHA has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a serious risk to the rights and freedoms of the data subjects who are subject of the

breach require to be reported externally in accordance with Clause 7.3 hereof.

7.2 **Internal Reporting**

CDHA takes the security of data very seriously and in the event of a breach will take the following steps:

- As soon as CDHA becomes aware that a breach has or may have occurred, the DPO must be notified of the breach or potential breach and be provided with all information available about the breach or potential breach;
- CDHA must seek to contain the breach by whatever means available;
- The DPO must consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with this clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

7.3 **Reporting to the ICO**

The DPO will require to report any breaches which pose a serious risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office ("**ICO**") within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach, or the ICO may instruct CDHA to notify those data subjects affected by the breach.

8. Data Protection Officer ("DPO")

8.1. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by CDHA with Data Protection laws. CDHA has elected to appoint a Data Protection Officer whose details are noted on CDHA's website and contained

within the Fair Processing Notice at Appendix 1 hereto.

8.2 The DPO will be responsible for:

8.2.1 Monitoring CDHA's compliance with Data Protection laws and this Policy;

8.2.2 Co-operating with and serving as CDHA's contact for discussions with the ICO

8.2.3 Reporting breaches or suspected breaches to the ICO and data subjects in accordance with clause 7 hereof.

9. Data Subject Rights

9.1 Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to a copy of the personal data held about them by CDHA, whether in written or electronic form.

9.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to CDHA's processing of their data. These rights are notified to CDHA's tenants and other customers in CDHA's Fair Processing Notice.

9.3 **Subject Access Requests**

Data Subjects are permitted to a copy of their data held by CDHA upon making a request to do so (a Subject Access Request) free of charge. Upon receipt of a request by a data subject, CDHA must respond to the Subject Access Request within one month of the date of receipt of the request.

9.3.1 CDHA must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.

9.3.2 Where the personal data comprises data relating to other data subjects, CDHA must consider: (i) whether it has the consent of

those other data subject to release their data; or (ii) whether it would be reasonable in all the circumstances to release their data. If CDHA does not have consent and does not consider it reasonable to release this data, then steps must be taken to remove or redact any third party data from the information to be released to the requester.

9.3.3 Where CDHA does not hold the personal data sought by the data subject, CDHA must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

9.4 **The Right to be Forgotten**

9.4.1 A data subject can exercise their right to be forgotten by submitting a request in writing to CDHA seeking that CDHA erase the data subject's Personal Data in its entirety.

9.4.2 The right to be forgotten is not an absolute right. Where CDHA is legally bound to retain certain information, or it has a legitimate interest to retain information, it is entitled to refuse a request to be forgotten. Each request received by CDHA will require to be considered on its own merits. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.4 and will respond in writing to the request. Where a request is refused, the DPO will explain the rationale of this decision when responding to the requester.

9.5 **The Right to Restrict or Object to Processing**

9.5.1 A data subject may request that CDHA restrict its processing of the data subject's Personal Data, or object to the processing of that data.

In the event that any direct marketing is undertaken from time to time by CDHA, a data subject has an absolute right to object to processing of this nature by CDHA, and if CDHA receives a written request to cease processing for this purpose, then it must do so immediately.

9.5.2 Each request received by CDHA will require to be considered on its own merits. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

10. Privacy Impact Assessments ("PIAs")

10.1 These are a means of assisting CDHA in identifying and reducing the risks that our operations have on personal privacy of data subjects.

10.2 CDHA shall:

10.2.1 Carry out a PIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using Special Categories of Personal Data, or the implementation of a new IT system for storing and accessing Personal Data which may give rise to security risks, or any processing which requires Personal Data to be transferred to a location outside of the European Economic Area; and

10.2.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data.

10.2.3 CDHA will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five
(5) working days.

11. Archiving, Retention and Destruction of Data

CDHA cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. CDHA shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified at Appendix 5.

Appendices

Appendix 1- Fair Processing Notice;
Appendix 2 - Data Retention

CDHA
Cathcart & District Housing Association

Appendix 1 - Fair Processing Notice for Cathcart & District Housing Association – All Relevant Parties

How we use your information

Cathcart & District Housing Association is known as "Controller" of the personal data provided to us and is required to make sure all personal information is handled and kept carefully in line with General Data Protection Regulations (GDPR).

The information we collect from you will primarily be basic personal contact details required to carry out our major functions as a social housing provider, however there are occasions where we are required to collect data of a more sensitive nature and this will be treated with the appropriate level of confidentiality.

We may collect the following personal information about you.

- Personal details: name, addresses, date of birth
- Contact details: home phone number, mobile phone number and email address
- Further details: NI number, gender, ethnicity, disability, medical details, marital status, signature, unacceptable behaviour warnings
- Household composition: details of existing accommodation arrangements and family members seeking accommodation with the applicant
- Tenancy Details: start and end dates, rent paid, under/over payments
- Payment details: bank account details, 3rd party payment details
- Repairs: repairs requested, access details, completion dates
- Pseudonymised data: CDHA customer account numbers, rent/factors reference number, share membership number
- Purchase details: solicitors details
- Employment: benefit/council tax status and payments, employment history, education history, tax code, trade union membership
- Employment application details, asylum status, criminal record declaration
- Location: IP address
- Images: event photographs, CCTV images
- Voice recording on our voicemail and office telephones

We may also record factual information whenever you contact us or use our services, as well as information about other action we take, so we have a record of what happened.

We need to know your personal data to provide you with the housing services you have engaged with us to provide, and to communicate effectively with all data subjects as required by the Scottish Housing Regulator.

We need your personal information to allow us to be able to:

- Process and manage housing applications
- Sign up new tenants to suitable properties
- Carry out duties highlighted in contract as landlord
- Meet our legal obligations including information that we have to provide to regulators and statutory authorities
- Adhering to statutory regulation and providing yearly returns and statistics
- Reply to enquiries and contact all customers when required
- Provide an efficient maintenance service ensuring our properties and repairs are of an appropriate standard
- Issue invoices and follow up contact where required
- Deliver a value for money factoring facility for owners
- Ensure we have enough resources to carry out all functions
- Managing payments from you or your account and for accounting purposes
- Process your job application
- Prevention and detection of crime
- Perform or assist in debt recovery or court actions
- Facilitate any necessary legal proceedings
- Issue satisfaction surveys, newsletters and service information
- Administer lets and training sessions

Sharing your Information

All personal data we process is processed by our staff in the UK. We sometimes need to share personal information with other organisations, however where this is necessary, we are required to comply with all aspects of GDPR. Even when this is required, we only share data within the European Union (EU). We do not give anyone else access to your information in return for payment, for their marketing and commercial purposes.

Cathcart & District Housing Association may enter into partnerships with other organisations such as local authorities and the police. For example, we may join a partnership to help prevent and control anti-social behaviour. We will enter into a formal data sharing agreement to govern the process and ensure it is lawful. That agreement will be approved by our Data Protection Officer before it is implemented. The types of organisations we may share with in these instances are the following

- Glasgow City Council
- Community Safety Glasgow
- Other landlords
- Solicitors
- Trustees
- Sheriff Officers

We are also required to share information with statutory bodies governing finance and housing industries, for auditing and inspection purposes. However this will be restricted to the actual information required from the association and will be mainly viewed within the association, with strict permission set on our electronic file system

to ensure use is controlled. We will also encrypt and limit the content of any files that do have to be sent either electronically or otherwise.

We will share specific and relevant information with law enforcement, government or public bodies and statutory agencies where we are legally required to do so in order to aid:

- The prevention or detection of crime and fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax or duty owed to customs and excise
- Sharing in relation to physical or mental health of an individual, where disclosure is required to protect them or others from serious harm
- Sharing in connection with legal proceedings
- Research and statistical purposes

Cathcart & District Housing Association remains responsible for the fair and lawful processing of all personal data shared with suppliers. Unless we have requested your specific consent, we only share information with other external organisations or agencies that we have a signed agreement to do so with ensuring as data processor, all data they manage remains compliant to GDPR.

Contractors and suppliers

We may share your personal information with our suppliers who provide a service to you, or who provide services on our behalf. The data shared is the specific information the supplier requires to carry out their task, as well as any information that ensures we fulfil our health and safety obligations to the people carrying out the task. We may share this information with the following organisations:

- Maintenance contractors and suppliers
- Printing and mail distribution
- Customer surveys
- Insurers
- Banks
- Payment card, direct debit and billing solutions
- Document storage and archive scanning

In order to ensure all tenants have the required utilities available when they sign up to a tenancy with Cathcart & District Housing Association, we may also provide names and addresses, forwarding addresses, contact details and tenancy dates to utility providers.

Special Category Data

There are certain occasions where it will be necessary to perform our functions as a social housing landlord for us to share information containing special categories of data. Currently we would only ever share the following type of this more sensitive information:

- Racial or ethnic origin: Shared with statutory bodies and reported on as a statistical breakdown of housing or job applicants only, not including any actual personal data.

Third Party Access

Any third party who Cathcart & District Housing Association gives access to our electronic files is therefore called a Data Processor because they are processing Data on behalf of the Association. Although the Data Controller and Data Processor are two separate entities, we are required to ensure all third party access is given in compliance with all GDPR principles, and to this affect will have a third party access agreement in place.

The following organisations may be given controlled access to our electronic data for reasons of security, maintenance, or any specific purposes outlined in their third party agreement.

- IT maintenance/support contractors
- Specialist housing software providers
- User and file system auditing software provider

Power of Attorney

If you wish anyone to deal with your affairs on your behalf please find the specific consent form for this on our website or request this from our office. This allows you to request a named person permission to discuss specific or all of your personal data with the Association as required.

We will not share your personal information with anyone who claims to represent you unless we are satisfied that you have appointed them or they act in some recognised official capacity. There may be a delay to us dealing with requests whilst we confirm the caller's identity, or check that we have your approval to deal with them.

Violent or abusive behaviour

If you are violent or abusive to Cathcart & District Housing Association staff, customers, or other residents, we may decide to place a "warning marker" on your customer record in order to protect Cathcart & District Housing Association colleagues.

If we do this we will write and tell you why and you will have the right to appeal against our decision as per our Unacceptable Behaviour Policy. We will share this information with our partners, for example our contractors, Fire & Rescue Service in order to protect their colleagues too.

How we store your personal information

We are committed to holding your personal information securely. This means only those of our colleagues and contractors that need to see it have access.

Unless you pay your bills using direct debit we will not usually retain your payment details. Whoever pays your bills will have to give us the payment card details each time they make a payment.

If we store your personal information and can do so solely on computers we will, however there will be cases where we have paper copies instead, or in addition to this. All computers are kept in a secure location and are password protected, with unusual and unauthorised access monitored by specialist auditing software and our electronic files kept on shared network accessed by our computers are controlled by strict access permissions so data is only available to those who need to use it. Paper files containing personal information may be kept in drawers, cabinets or rooms.

Our computer systems are located in our offices in Cathcart but we occasionally use computers and laptops offsite, however they will at all times remain secure and under our control.

We will keep your personal details for no longer than necessary. Once the information is no longer required for the lawful purpose for which it was obtained it will be destroyed.

More information on the document retention schedule adopted by the Association can be found in the National Housing Federations most recent guide to document retention available online at https://www.housing.org.uk/resource-library/browse/document-retention-and-disposal-for-housing-associations/

Your rights

If at any point you believe that information we hold is incorrect you may request to see it, have it corrected or deleted. You are entitled to request a copy of any personal data we hold of yours.

You have the right to ask us not to process all or part of the personal information we have received, however we may be unable to provide our service to you if we are unable to record and process certain details.

If you wish to complain about how we have handled your data you can contact our Data Protection Officer who will investigate the matter on your behalf. If you are not satisfied with our response you may submit a formal complaint to the Information Commissioners Office.

As of 11th November 2019, Cathcart & District Housing Association is deemed to be a Public Authority under the Freedom of Information (Scotland) Act 2002 and is, therefore, required to appoint a Data Protection Officer (DPO). We have engaged with RGDP LLP (www.rgdp.co.uk) to act as our Data Protection Officer.

To contact them, please email info@rgdp.co.uk. Please also copy us in at: info@cathcartha.co.uk.

Appendix 2 – Data Retention

How long we will keep your information

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

We will generally keep your information for the following minimum periods:

Applications for accommodation	Duration of Tenancy
Housing Benefits Notifications/Universal Credit Notifications	Duration of Tenancy
Tenancy files	Duration of Tenancy
Former tenants' files (key info)	Duration of Tenancy unless debt left on account
Third Party documents re care plans	Duration of Tenancy
Records re offenders. Ex-offenders (sex offender register)	Duration of Tenancy
Lease documents	5 years after lease termination
ASB case files	5 years/end of legal action
Membership records	Permanently
Personal files including training records and notes of disciplinary and grievance hearings	6 years after employment ends. To cover the time limit for bringing any civil legal action, including national minimum wage claims and contractual claims
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of the redundancy
Application forms, interview notes	6 months date of interviews for unsuccessful applicants. Successful applicants' documents should be transferred to personal file.
Documents proving the right to work in the UK	Duration of employment.
Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies.
Payroll (including Income Tax, NI returns, correspondence with tax office, wages/salary records, expenses and bonuses)	6 years from termination date
Retirement benefits schemes – notifiable events, e.g. relating to incapacity	6 years from termination date
Pensioners records	6 years from termination date
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	6 years from termination date
Parental Leave	18 years

Statutory Sick Pay records, calculations, certificates, self-certificates	6 years from termination date
Wages/salary records, expenses, bonuses	6 years
Records relating to working time	2 years from the date they were made
Accident books and records and reports of accidents	3 years after the date of the last entry
Health and Safety assessments and records of consultations with safety representatives and committee	During employment
Health records	During employment
Board Members Documents	Permanently
Documents relation to successful tenders	5 years after end of contract
Documents relating to unsuccessful form of tender	6 months after notification and standstill period expires and if no challenges received. If challenge received retain for 5 years after notification.
Board meetings/residents' meetings	Permanently
Minute of factoring meetings	Duration of appointment

After which this will be destroyed if it is no longer required for the reasons it was obtained.