CROYDON CHURCHES HOUSING ASSOCIATION
and
CCHA DEVELOPMENTS LIMITED

GROUP DATA PROTECTION POLICY

Contents

1. Introduction

2. Policy Statement

3. Roles and Responsibilities

4. What Personal Data do we hold?

5. Right of Access to Personal Data (Subject Access)

6. Data Security

7. Transfer to Third Parties including international transfers

8. Accuracy of Personal Data

9. Right of Erasure

10. Training and Support

Appendix 2 Procedure for Handling Requests to Exercise Individual Rights (Subject Access Requests)

Appendix 3 Data Privacy Impact Assessments Procedure

Appendix 4 Data Breach Procedure

Appendix 5 Data Retention Guidance

Appendix 6 CCTV Procedure

Appendix 7 Procedure for Complaints Relating to Individual Rights Requests

Appendix 8 Glossary of Terms

1.0 Introduction

1.1 Croydon Churches Housing Association (ccha) collects, stores and processes data about its residents, employees, and other individuals to deliver the services people need and expect from us.

1.2 This document sets out how the Group will comply with its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and how it will manage the personal data that it holds.

1.3 Relationship with other policies and procedures

1.3.1 This policy is underpinned by other policies and procedures within the Group, they include: -

- CCTV Procedure
- Subject Access Request Procedures
- Data Breach Procedures
- Document Retention Procedures and (adopted) NHF Retention Schedule
- Data Protection Impact Assessment Toolkit and Form (DPIA)
- Privacy Notices and Website Privacy Statement
- Employee Handbook
- Data Sharing or Processing Agreement (DSA or DPA) (with 3rd parties)
- Departmental Compliance Statements

1.4 This policy applies to all employees, Board members, Committee members, agency workers, contractors and third parties processing personal data on behalf of CCHA.

2.0 Policy Statement

ccha is a Data Controller and processes personal data. As such it is required to comply with the UK GDPR and Data Protection Act 2018 (the Act).

ccha is regulated by the Regulator of Social Housing, which as part of the Governance and Financial Viability Standard of the Regulatory Framework, requires all registered providers of social housing to adhere to all relevant law. This reinforces the need to comply with the UK GDPR and the Act.

To comply with the UK GDPR and the Act, ccha is committed to:

- Processing personal data lawfully, fairly and transparently.
- Collecting and using personal data only for specified and legitimate purposes.
- Ensuring personal data is adequate, relevant, accurate and limited to what is necessary.
- Retaining personal data only for as long as necessary.
- Protecting personal data through appropriate security measures.
- Respecting and supporting the rights of individuals.
- Embedding privacy by design and by default in our activities.
- Demonstrating accountability for compliance with data protection legislation.

UK GDPR defines personal data as “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”.

The UK GDPR also identifies the following special category data relating to an individual

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (if used to identify someone)
- Health data (physical or mental)
- Sex life
- Sexual orientation

These categories of data are considered more sensitive under UK GDPR and are subject to additional conditions before they may be processed.

3.0 Roles and Responsibilities

Organisations that decide how and why personal data is processed are known as “data controllers”. ccha is a data controller, as are its operating subsidiaries.

Every employee and Board and Committee member is responsible for complying with this policy and supporting the Group's compliance with data protection legislation. Individuals must ensure that personal data is handled lawfully, fairly, securely and confidentially; only accessed, used or shared where necessary and authorised; kept accurate where appropriate; and managed in accordance with the Group's policies, procedures and retention requirements. Any actual or suspected data breach,

inappropriate disclosure or misuse of personal data must be reported promptly in line with the Group's Data Breach Procedure. Specific responsibilities are set out below.

In order to meet the accountability requirements, set out in the UK GDPR, ccha must be able to demonstrate compliance with the Data Protection Principles, by:

- Maintaining a Governance Structure
- Maintaining a Data Protection Policy and Process Framework
- Embedding Data Protection into ccha's operations
- Maintaining a training and awareness programme
- Managing Information Security and Cyber risk
- Managing risks associated with the use of third parties
- Publishing relevant notices where Personal Data is collected
- Responding to requests and complaints from individuals Integrating Data
- Protection by Design and Default into ccha's operations using Data Protection Impact Assessments
- Maintaining a Data Breach recording, investigation and reporting process
- Monitoring Data Handling Practices

3.1 Named Data Protection Contact

3.1.1 The Company Secretary is ccha's named Data Protection Lead throughout the policy and appendices.

3.1.2 The named Data Protection contact has responsibility for advising on compliance, monitoring compliance, supporting DPIAs, acting as a point of contact for the ICO and individuals exercising their rights, and reporting significant data protection risks or breaches:

3.1.3 The Group has assessed its obligations under UK GDPR and has determined that it is not currently required to appoint a Data Protection Officer. This decision is kept under review.

3.2 SMT and Management roles

3.2.1 All in SMT or equivalent management roles (management) are responsible for ensuring compliance with this policy within their areas of responsibility. As Information Asset Owners or Information Asset Administrators they also ensure that information asset records are maintained where applicable.

3.2.2 Management will carry responsibility for determining the access required to systems processing personal data by their team members, ensuring that each team member has access to the right systems and applications, has the right level of permissions, has the right equipment, and receives the required training to use the IT service properly.

3.2.3 Management will also be responsible for ensuring good data protection within their teams. They are responsible for ensuring that there is a legal basis for processing identified and, if processing special category data that there is the correct condition for that processing; that data is used only for the purposes for which it is provided; and that the data is accurate. They should regularly review and update the Information Asset Register and manage any Data Breaches or potential Data Breaches. Managers should ensure that their SMT teams complete mandatory data protection training.

3.2.4 Management will be responsible for ensuring that where data is removed from the premises, this is only done when necessary and that arrangements are in place to ensure that the data is kept secure throughout the time that it is removed from the premises.

3.3 All Staff Members

3.1.1 All staff members are expected to comply with this policy and its accompanying appendices, ensuring that all incidents and/or breaches of this policy are reported in accordance with ccha's data breach guidance.

3.4 Engaging Third Parties

3.4.1 Third parties such as partners, public and private organisations or contractors with whom Croydon Churches shares personal data or who hold personal data on the organisation's behalf will need to enter into and adhere to formal arrangements or contractual obligations with the organisation, incorporating the principles of this policy and the requirements of the legislation. A Data Sharing Agreement (DSA) will be required for all controllers, and a Data Processing Agreement (DPA) may be required for processors of ccha personal data where personal data sharing arrangements are not clarified or specified in the contract. These should be concurrent for the life of the contract, include consideration of the contractor's responsibility for personal data once the contract has ended, and be subject to review and amendment when the contract is renewed or there is a change to the personal data shared.

4.0 What Personal Data do we hold?

4.1 The Group will hold personal data in line with this policy. This includes but is not limited to:

- Employees
- Job applicants
- Residents and those who live with them
- Applicants for tenancies
- Board and Committee Members
  - Individual contractors and consultants
  - Customers and potential customers of market sale properties
  - The former members of the above categories, in line with the retention schedule

4.2 All Managers or equivalent role will ensure that they are aware, in general terms, of the personal data they store and process on individuals and that the provisions of this policy are followed in relation to such personal data.

4.3 Data Subjects have a right to view personal data about themselves. In specific circumstances this may extend to other individuals. They are entitled to know:

- What data is held or otherwise processed about them;
- The purpose of the processing;
- The recipients or categories of recipient to whom the personal data have or will be disclosed;
  - Where possible, the envisaged period for which the personal data will be stored;
  - The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data;
  - The right to lodge a complaint directly with ccha or escalate a complaint with the ICO;
  - Where the personal data is not collected from the data subject, any available information as to their source.

4.3.1 Data that is not about an individual but about our aggregated customer data is covered by Access to Information (STAIRs) and further information is on our website FAQ page.

4.4 The Group will only collect and process personal data if one of the conditions set out in Article 6 of the UK GDPR have been satisfied. We have set out each of the conditions under Article 6 of the UK GDPR that could potentially be relevant for the Group's activities:

- The consent of the resident, employee or stakeholder is obtained prior to the processing of personal data. Consent must be freely given; it must also be specific and informed. In practice this means that wherever possible consent should be obtained in writing and signed by the subject with clear wording in plain English explaining precisely what they are agreeing to. Where written consent is not possible, any clear affirmative action can be given but the terms of the consent must be clearly given to the subject and a written record of the consent kept;

- Processing is necessary for the performance of a contract to which the resident, employee or stakeholder is party or to take steps at the request of the resident, employee or stakeholder prior to entering the contract;
- Processing is necessary for compliance with a legal obligation to which the Group is subject;
- Processing is necessary to protect the vital interests of the resident or employee or of another natural person; and
- Processing is necessary for the purposes of the legitimate interests pursued by the Group or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the residents or employee which require protection of personal data, in particular, where the data subject is a child.

4.5 Personal data – especially special category data, about residents, employees and stakeholders is only accessed and shared only where there is a legitimate business need. This may involve sharing personal data between individuals in different departments. The need for staff access to personal data is set out in individual job descriptions and ccha policies.

4.6 The Group will only collect and process special category data if one of the conditions set out in Article 9 of the UK GDPR has been satisfied. Alternatively, where there is an exemption under Article 9, along with a specific Schedule 1 paragraph (of the Data Protection Act 2018[i]) that applies to the purpose and an appropriate policy document is in place. These are both in addition to satisfying one of the conditions in Article 6 of the UK GDPR. We have set out each of the conditions under Article 9 of the UK GDPR that could potentially be relevant for the Group's activities:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes. Consent must be freely given;
- 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 have been made manifestly 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; and
- 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.

4.7 Children

4.7.1 The Group understands that children need protection when we are collecting and processing their personal data and that their data must be processed with particular care and using age-appropriate privacy information.

4.7.1 When we rely upon 'legitimate interests' as the basis for processing, we balance the Group's legitimate interests in processing the personal data against the interest and fundamental rights and freedoms of the child and we will complete a Legitimate Interest form.

4.7.3 When relying on 'necessary for the performance of a contract' we consider the child's competence to understand what they are agreeing to, and to enter into a contract.

5.0 Right of Access to Personal Data

5.1 All residents, employees, stakeholders and any other identifiable individual whose personal data is processed by ccha have a right to ask the Group, under the UK GDPR, for personal data held about them and this section details the personal data they are entitled to see under UK GDPR.

5.2 Individuals' rights of access under the UK GDPR are set out in the Group's Subject Access Request Procedure

6.0 Data Security

6.1 The Group will take the following steps to ensure that personal data is kept securely:

- System for Access: Access to personal data will be restricted to specified individuals based on appropriateness, for example, employee personnel files will only usually be accessed by the individual's manager, Director or the HR Department.
- If the file or contents within it must be accessed by others, such as appeals or grievance sub committees, the arrangements to ensure confidentiality and compliance with this policy will be made known at the time.
- **Passwords**: Confidential personal data held on computer will in all cases be password-protected, and the password will only be released to individuals who are authorised to access the personal data. The Group will ensure staff receive our UK GDPR related training and are informed to deploy complex passwords, ensuring the best possible defence against data theft.
- **Training**: All staff that are given authority to access personal data will be appropriately trained so that they are aware of the principles of data protection and how to work in accordance with best practice for processing personal data.
- **Transfer off Site**: When personal data is transferred off site, it must be kept secure.
- **IT Systems**: The Group will take all reasonable measures to ensure that its IT systems are secured. This will include the control and security of the network in circumstances where third party contractor or suppliers legitimately need to access our systems. Requests in these circumstances will be referred to the Director of Finance and Resources (DoFR) for approval.

7.0 Transfers to Third Parties

7.1 If the Group is asked to transfer personal data to third parties such as the police, social services and other bodies with legal authority such as the Department for Work and Pensions, such transfers will only be completed in line with our policy and accordance with data protection legislation.

7.2 Approval in such circumstances will be made by a middle manager, director or equivalent role.

7.3 The Group will confirm the identity of any third party and always seek requests in writing.

7.4 In emergency situations, personal data will only be shared over the phone when the officer concerned is confident, they know to whom they are speaking and that disclosure is appropriate.

7.5 The Group will exercise particular care in relation to disclosure of special category data and will only disclose to third parties in limited circumstances. Usually, the individual concerned should have given consent (e.g. disclosure of health data to a doctor or the social services) or it should be necessary for the exercise of statutory functions.

7.6 The Group will disclose personal information if the disclosure is being made to investigate crime and non-disclosure would prejudice the investigation, e.g. to the police. In these circumstances, the Group will make a note of the reason why the disclosure was made to the third party and keep this on the individual's file. Personal data will only be disclosed only on receipt of a written request.

7.7 International Transfers and Overseas Processing of Personal Data

The Group recognises that certain suppliers and service providers, including cloud-based technology providers, e.g. Microsoft and other authorised third parties, may process, access, host, store or transfer personal data outside of the UK while providing services to the Group

7.7.1 The Group will not transfer personal data outside the United Kingdom, nor permit personal data to be processed outside the United Kingdom, unless the requirements of applicable Data Protection Legislation, including the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025 ("DUAA"), as amended from time to time, are satisfied and appropriate safeguards are in place to ensure that the rights and freedoms of data subjects are protected.

7.7.2 Any international transfer or overseas processing of personal data undertaken by, or on behalf of, the Group may only take place where one or more of the following conditions is met:

- The recipient country, territory or international organisation is the subject of UK adequacy regulations recognised by the UK Government;
- The transfer is made subject to an approved International Data Transfer Agreement ("IDTA"), the UK Addendum to the EU Standard Contractual

Clauses, or any successor transfer mechanism recognised under UK Data Protection Legislation, together with a Transfer Risk Assessment ("TRA") where required;

- The transfer is made under approved Binding Corporate Rules ("BCRs") or another approved certification or code of conduct mechanism recognised under UK Data Protection Legislation;
- The transfer is necessary under one of the specific derogations or exemptions permitted by UK Data Protection Legislation;
- The transfer otherwise complies with any international transfer provisions, adequacy mechanisms, or recognised safeguards introduced, amended or replaced by the DUAA or subsequent legislation.

7.7.3 Where the Group uses cloud-based or software-as-a-service providers, personal data may be processed from locations outside the United Kingdom for operational, support, security, resilience, business continuity, or service delivery purposes. In such circumstances, the Group will ensure that appropriate contractual, technical, and organisational measures are implemented to maintain an equivalent level of protection for personal data.

The Group will maintain records of international transfers where required and will periodically review the safeguards relied upon to ensure ongoing compliance with applicable Data Protection Legislation.

8.0 Accuracy of Personal Data: Right of Rectification

8.1 Any individual whose personal data we process may challenge the personal data held by the Group on their file if they believe it to be incorrect and can provide evidence to support this.

8.2 The right of rectification under the UK GDPR (Article 16) entitles the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data concerning them.

9.0 Right of Erasure, Restriction on/Objection to Processing and Withdrawal of Consent

9.1 Under the UK GDPR the rights of data subjects are extended to give individuals more protection and greater control over their personal data.

9.2 The right to erasure is also known as 'the right to be forgotten'. This enables any individual whose personal data we process to request the deletion or

removal of personal data where there is no compelling reason for its continued processing by the Group.

9.3 The right to erasure does not provide an absolute 'right to be forgotten'. Individuals only have a right to erasure where:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- Where the individual withdraws consent and the legal basis for processing relied on such consent.
- Where the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the UK GDPR).
- The personal data must be erased to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

9.4 The Group can refuse to deal with a request to erase where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To enable functions designed to protect the public to be achieved, e.g. government or regulatory functions;
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research historical research or statistical purposes;
- The exercise or defence of legal claims; or
- Where the organisation has an overriding legitimate interest in continuing with the processing.

9.5 Restriction on Processing

9.5.1 A data subject has the right to require a controller to stop processing their personal data. When processing is restricted, the Group is allowed to store the personal data, but not further process it.

9.6 The Group will be required to restrict the processing of personal data in the following circumstances:

- Where an individual (usually but not solely, employees or residents) challenges the accuracy of the personal data, we must restrict processing until we have verified its accuracy.
- Where an individual has objected to the processing (where it was necessary for the purpose of legitimate interests), and we are considering whether our legitimate grounds override those of the individual.
- When processing is unlawful and the individual requests restriction instead of erasure.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.
- If we have disclosed the personal data in question to third parties, we must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

9.7 We must inform individuals when we decide to remove the restriction giving the reasons why.

9.8 Objection to Processing

9.8.1 Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public tasks/exercise of official authority; direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

9.8.2 The only category relevant to the Group is where we process personal data for the purposes of our legitimate interests. In that case, where an individual (resident or employee) objects, we must stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual (via a legitimate interest test); or
- The processing is for the establishment, exercise or defence of legal claims.

9.9 Withdrawal of Consent

9.9.1 An individual has the right to withdraw consent at any time.

If the basis on which personal data is being processed is the consent of the individual, then that processing must stop.

9.9.3 It may be that another reason for processing can be relied on such as legitimate interests.

9.9.4 In practice a withdrawal of consent is likely to be accompanied by a request to erase in which case the Group will need to rely on one of the other exceptions to erasure, e.g. overriding legitimate interest.

10.0 Training and Support

10.1 We will work to communicate and embed the principles of Data Protection in everything we do, ensuring all staff are made aware of their responsibilities under the UK GDPR and are given access to training and guidance, in response to evolving best practice and learning.

10.2 We will maintain relevant and practical procedures for staff on issues such as the data subject's right over access, objection and rectification, document retention, and data security.

Version History	
Policy Name	Group Data Protection Policy
Lead Officer	Company Secretary (named Data Protection Lead)
Date of Issue	August 2026
Review Date	Updated August 2026 in line with the Data Use and Access Act (DUAA) Review August 2029
Regulation based on	UK General Data Protection Regulation (UK GDPR)
Policy Replaced	Group Data Protection Policy reviewed 2024
Version code	2

[i] ccha considers The Data Protection Act 2018 and all related legislation relevant to this policy and appendices

Appendix 2: Procedure for Handling Requests to Exercise Individual Rights under UK GDPR including Subject Access Requests:

1. Purpose and Scope

1.1 This procedure supports the Group Data Protection Policy by setting out how requests from individuals to exercise their rights under UK GDPR will be handled. It applies to requests received from residents, customers, colleagues, former colleagues, applicants, service users and other individuals whose personal data is processed by the organisation.

1.2 The procedure should be read alongside the Group Data Protection Policy, relevant privacy notices and associated procedures. It does not repeat the data protection principles or wider legal responsibilities, which are covered in the main policy.

2.0 Who can make a request for their data under the UK GDPR?

2.1 Data subjects are entitled to make requests about the personal data ccha and cchadl hold on them including special category data. Anyone whose data is processed by ccha or cchadl is entitled to exercise their data rights.

3.0 What types of requests could we receive?

3.1 Right to Access (Subject Access Request)

3.1.1 A data subject can request a copy of all the personal data we hold about them, including special category data but not information relating to another data subject (unless the information is also about them or they are authorised to act on behalf of someone else).

3.1.2 A data subject can make a request via a third party such as a solicitor, family member or friend. In such situations we must receive in writing confirmation from the data subject that the third party is acting on their behalf or a power of attorney must be in place.

3.1.3 Children have the same right of access to their data as adults. However, children need to have the maturity to understand and exercise these rights. Requests involving children must be considered on a case-by-case basis, taking account of the child's age, maturity and ability to understand the request.

3.1.4 In responding to the request, we must also provide them with the following information:

- The purposes of the processing;
- The categories of personal data concerned;

- The recipients or categories of recipient to whom the personal data have been or will be disclosed;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- Their rights of rectification, erasure, restriction of processing and to object;
- The right to lodge a complaint with the ICO;
- Where the personal data is not collected from the data subject, any available information as to their source;
- A statement about our use of automated decision-making, including profiling, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3.1.5 We must provide the data held at the time of the request unless changes need to be made as part of our normal course of business between receiving the request and collating the information. It is an offence to amend or delete data which would not otherwise have been amended or deleted to prevent its disclosure.

3.1.6 Any information we provide must be concise, transparent, intelligible and easily accessible. It is therefore important that the information can be understood by an average person.

3.1.7 Please note, it is a criminal offence in certain circumstances and in relation to certain information to require an individual to make a subject access request. Please see ICO website for more information.

3.2 Right to Rectification

Data subjects can request that inaccurate personal data is corrected, and incomplete personal data is completed. In responding to the request, we must:

- If requested by the data subject, restrict processing while the data's accuracy is contested and being checked. (Please see section 4.4 below). However, even if the data subject has not requested it, as a matter of good practice, we will restrict processing while the data is being checked where possible;
- Take reasonable steps to satisfy ourselves that the data is accurate and to rectify the data if necessary. In doing this, we will consider the arguments and evidence provided by the data subject;
- Keep a record of any original mistakes and how they have been resolved.

3.2.2 Please note that:

- Where the records reflect a matter of opinion, these are likely to be subjective, and it is difficult to determine accuracy. Opinions do not need to be corrected but it should be noted that it is an opinion and where appropriate whose opinion it is.

3.2.3 If we judge the information does not need amending, we must inform the data subject explaining our decision and their rights of recourse. See section 8.3 below).

3.3 Right to Erasure (Right to be Forgotten)

3.3.1 This is not an absolute right and only applies in certain circumstances. Individuals have the right to have their personal data erased only if:

- The data is no longer necessary for the purpose(s) it was originally collected;
- The lawful basis for processing the data was:
  - Consent and the data subject has withdrawn consent:
  - Legitimate interest and the data subject objects to the processing of their data and there is no overriding legitimate interest to continue.
- Processing was for direct marketing purposes, and the data subject has objected;
- The data has been processed unlawfully;
- There is a legal obligation for us to comply to the request to exercise the right to erasure;
- The data has been processed to offer information society services to a child.

3.3.2 The Right of Erasure does not apply if the lawful basis for processing the data was:

- to comply with a legal obligation,
- to carry out a task in the public interest, or
- for archiving purposes in the public interest, scientific research, historical research or statistical purpose.

It also does not apply if a person was exercising their right to freedom of expression or information.

3.3.3 In responding to the request, we must ensure that:

- Reasonable steps are taken to erase data from both backup and live systems. Any delay in the erasure from the backup system is only acceptable if the information is “beyond use” and the necessity of the delay should be explained to the data subject;
- Information is erased from public online environments;
- Extra weight is given to requests about children.

3.4 Right to Restrict Processing

3.4.1 This right is not absolute and only applies in certain circumstances. Data subjects can only exercise this right if they have a particular reason for wanting

the restriction. This may be about the information held or how it is processed. Normally a restriction will be in place for a certain period.

Data subjects only have the right to restrict the processing of their personal data if:

- They contest the accuracy of their data, and it is being verified;
- The data has been unlawfully processed, and the data subject has requested that the processing of data is restricted instead of erased;
- We no longer need the data, but the data subject needs us to keep it to establish, exercise or defend a legal claim;
- The data subject has objected to us processing their data under article 21 (the Right to Object see paragraph 4.6 below) and we are considering whether our legitimate interest override the rights of the data subject.

3.4.2 In responding to the request, we must ensure that:

- All letters, emails, documents etc are moved to a restricted processing file which can only be accessed by the Leadership Team, named Data Protection contact and System Administrator(s).
- Any relevant data is removed from our website;
- The data is made unavailable to users;
- No processing is undertaken other than storage unless:
  - The data subject gives consent;
  - It is needed to establish, exercise or defend a legal claim;
  - It is used to protect the rights of another person;
  - It is for the reasons of important public interest.

3.4.3 If we judge the data to be accurate or that our legitimate grounds for processing the data override those of the data subject, we can lift the restriction. Before we do this, we must inform the data subject explaining our decision, their right to rectification and right to object and their way to recourse. (See section 7.3 below).

3.5 Right to Data Portability

3.5.1 Data subjects have the right to move, copy and transfer personal data easily from one IT environment to another in a safe and secure way. The data subject can either receive the data or request that we transfer it directly to another controller. This right only applies if:

- The lawful basis for processing is consent or performance of a contract;
- The processing is being carried out by automated means (paper files are not covered by this right);

- The data was provided by the data subject (but this includes data resulting from observations of an individual's activities (e.g. search history but not any analysis carried out by the data controller).

3.5.2 Please note that pseudonymous data is subject to the Right to Data Portability.

3.5.3 In responding to the request, we must ensure that:

- We consider if any third-party data is included and if so, whether the transfer would adversely affect the rights and freedoms of the third party. If the data was originally provided by the data subject this is unlikely to affect the third party's rights.
- In the cases of multiple data subjects (i.e. a joint bank account), all parties to the data have agreed to the portability request.
- The data is transferred in a structured, commonly used and machine-readable format. It is important that the most appropriate system is used taking account of these three requirements and that where possible interoperable formats should be used.
- Transfers to another controller are carried out whenever this is technically feasible and without hinderance (i.e. not putting in place a legal, technical or financial obstacles which would slow down or prevent the transmission). Unless there are legitimate reasons not to transfer the data i.e. doing so would adversely affect the rights and freedoms of others.
- The data is transferred by a secure means using passwords or other security measures to the correct person.

3.5.4 When we receive personal data from another controller, we must ensure that:

- The data is relevant and not excessive;
- We have a lawful basis for processing any third-party data and that this does not adversely affect the rights and freedom of that party;
- We delete any unnecessary data;
- We comply with all other UK GDPR requirements.

3.6 Right to Object

3.6.1 Data subjects have the right to ask that the processing of their personal data is stopped.

3.6.2 We must inform data subjects of their right to object at the time of our first communication with them when processing is for direct marketing, performance of a public task or legitimate interest.

3.6.3 There is an absolute right in relation to direct marketing (including direct marketing using profiling data). We must stop processing personal data for this process if we receive a request. We do not need to necessarily erase the individual's data

so long as we can just suppress their details to ensure that their preference is respected.

3.6.4 Individuals can also object if their data is being processed under the legal bases of:

- Performance of a public task
- Legitimate interest

Individuals can also object if their data is being used for scientific or historical research or statistical purposes but if suitable safeguards are in place, the objections are more likely to be made under legitimate interest or performance of a public task.

3.6.5 As the Right to Object is not an absolute right (except in respect of direct marketing), the data subject must give a specific reason why they are objecting. We can continue processing if:

- We can demonstrate compelling legitimate grounds which override the data subject's interests, rights and freedoms. But we need to consider the balance of the data subject's interests, rights and freedoms and our legitimate reasons.
- We are processing the data to establish, exercise or defend legal claims.

3.6.6 In responding to the request, we must ensure that, if:

- A legitimate ground for continuing to process data exists, we must inform the data subject explaining our decision and their rights of recourse. (See section 8.3 below).
- There is no legitimate ground, we stop processing and consider whether we should erase all the personal data held.

3.7 Rights in relation to Automated Decision Making and Profiling

3.7.1 Under UK data protection law, individuals have rights in relation to automated decision-making and profiling where decisions are made solely by automated means and produce legal effects or similarly significant effects on the individual.

3.7.2 Individuals have the right to:

- Request human review of an automated decision;
- Express their point of view;
- Challenge or contest the outcome of an automated decision;
- Receive meaningful information about the logic involved in the processing and the reasons for the decision;
- Object to profiling, particularly where it is used for direct marketing purposes.

3.7.3 Automated decision-making may be permitted where:

- It is necessary for entering into or performing a contract with the individual;
- It is authorised by law; or
- The individual has given explicit consent.
- Where special category data is involved, additional legal requirements and safeguards must be met.

3.7.4 Where automated decision-making is used, appropriate safeguards must be in place to protect the rights and freedoms of individuals, including mechanisms for human intervention, review and challenge.

3.7.5 Before introducing any process involving automated decision-making or profiling that may have legal or similarly significant effects on individuals, a Data Protection Impact Assessment (DPIA) must be completed and approved in accordance with the Group Data Protection Policy and DPIA Procedure.

3.7.6 Individuals must be informed, through privacy notices or other appropriate communications, where automated decision-making or profiling is used in the processing of their personal data and of the rights available to them.

How will we receive a request?

4.1 Data subjects can make a valid request to exercise their rights under UK GDPR either verbally, in writing, via social media or by completing our Subject Access Request (SAR) form. As there is no specific form of words which need to be used, it is important to be alert to when an individual is making a request and if in doubt to seek clarification.

4.2 We can ask for identification of the person requesting to exercise their request and this should be done if there are any doubts about the person's identity, but we need to make sure that the request is proportionate. We must inform the data subject as soon as possible that identification will be required.

4.3 If requests are received by third parties, we will require a letter of authority signed by our resident or staff in advance of any search. For example, a third party may be a solicitor, family member or person who has delegated authority.

5 What do I need to do when I receive a request?

5.1 All requests should be acknowledged in writing (usually by email), this is particularly important for requests made verbally as it enables us to verify the exact nature of the request. For Subject Access Requests, we can ask for clarification about the nature of the information required especially if we hold a large amount of data. Our SAR form is a supportive tool for the requester. Where the request is not clear or where identification in 4.2 has not been received, the SAR will be "paused" for clarification and communicated to the requester.

5.2 ccha's Data Protection Lead is the CoSec and must be informed of all requests. The named Data Protection contact will log the request on "Register of SAR and Other Right Requests" and ensure the request is responded to within the necessary timescale.

5.3 Any processors must be informed of the request as soon as possible and asked to action the request and provide written confirmation of doing so.

5.4 For Subject Access Requests: The output of a SAR will be communicated using secure electronic systems. Paper generated copies are not automatic and must be requested for each SAR. They will be made available for collection via a pre-arranged appointment and should be collected within three weeks of the request. A manager and/or the Data Protection Lead should review the documents and ensure references to any other data subject are redacted. The review must also remove any information we are not permitted to disclose, such as information about a police investigation or criminal prosecution.

5.5 Once the necessary actions have been taken, an outcome reply (and if necessary, paper printouts of the required documents) confirming what steps have been taken must be sent within one month of request being received and a copy saved. Only one copy is free, see section 8. The reply to a request should be in the same media as the request (i.e. if the person makes a request by email, our reply should be emailed) unless the data subjects agree for an alternative method of response. Data will be shared via a secure link in SharePoint or other secure system and made available for one month to download.

6 Are there certain timescales we must adhere to?

6.1 All SARs must be complied with without undue delay, and in any event within one calendar month of receipt. However, if additional information is required before handling the request (e.g.to verify the data subject's identity), the timeframe will be paused and resumed once this information has been received. This is calculated from the day the request is received (including weekends and bank holidays). If the corresponding date does not exist (i.e. 31st of March to April), the deadline is the last day of the month. However, if the response day is a weekend or bank holiday, the response must be sent on the next working day.

6.2 We can extend the response time by up to a further two months if the request is complex or we have received numerous requests from the same individual. We must inform the individual without delay and at least within one month of receiving the request why an extension is necessary. However, ICO guidance indicates that an extension is not reasonable if the request is manifestly unfounded or excessive, an exemption applies, or we have waited for proof of identity before considering the request.

7 Can we refuse to handle a request?

7.1 Where a request is manifestly unfounded, excessive or repetitive we can either:

- Request a "reasonable fee" to deal with the request (see below); or
- Refuse to deal with the request

7.2 We can also refuse to comply in certain circumstances with requests for:

- The Right to Erasure
- The Right to Object
- The Right of Rectification

(See relevant sections above)

7.3 Whenever we refuse to comply, we must inform the data subject of our decision without delay and within the 30-day period and explain:

- Our reasons for not acting;
- The data subject's right to complain to ccha's Data Protection Lead using our Data Rights Complaints Procedure
- The data subject's right to complain to the ICO at www.ico.org.uk or by calling 0303 123 1113;
- The data subject's ability to seek to enforce this right though a judicial remedy.

7.4 For Subject Access Requests only: The UK GDPR does not introduce an exemption due to the amount of data. Thus, just because a request means we have to process a large quantity of information about an individual does not mean that it can be treated as manifestly unfounded or excessive. However, the UK GDPR does permit us to ask them to specify the information required. If a data subject has received documentation through a previous SAR, our duty will be to provide the information added since the last request.

8 Can we charge a fee for processing?

8.1 In most cases, we cannot charge a fee. However, a "reasonable fee" can be charged to cover administrative costs, if the request is manifestly unfounded or excessive. If we decide a fee is justified, we need to inform the individual promptly. We do not need to comply with the request until we have received the fee.

If a paper copy is specified, one copy will be supplied free and made available for collection and shared only after identification has been verified.

If there is an agreement to post, postage would be by a secure method and, where a fee is being charged, it is payable in advance.

9 Organisation Policies and Procedures supporting this procedure are:

- Group Data Protection Policy
- Data Breach Procedure
- Data Protection Impact Assessment Procedure Form
- CCTV Procedure
- NHF Data Retention Schedule
- Electronic Equipment Procedure
- Privacy Notice and Website Privacy Information

10 Contacts

10.1 If you have any queries about this procedure, please contact the CoSec, ccha's Data Protection Lead.

11 Review

11.1 This Procedure will be reviewed every 3 years or on account of any relevant changes in law or guidance from the Information Commissioner.

11.2 We may carry out checks or audits from time to time to ensure that
the requirements of this procedure are being followed.

Version History	
Procedure Name	Procedure for handling requests to exercise individual rights under UK GDPR (including Subject Assess Requests)
Lead Officer	Company Secretary (named Data Protection Lead
Date of Issue	August 2026
Review Date	August 2029
Regulation based on	General Data Protection Regulation (UK GDPR) and Data (Use and Access) Act 2025 (DUAA)
Parent Policy	Group Data Protection Policy 2026
Version Code	2

Appendix 3: ccha Data Protection Impact Assessment Toolkit and Form

1. Introduction

1.1 Under UK data protection law, organisations are required to carry out a DPIA where processing is likely to result in a high risk to individuals' rights and freedoms. A DPIA is required where processing is likely to result in high risk, particularly where there is:

- new or intrusive technology;
- large-scale processing;
- special category or criminal offence data;
- systematic monitoring;
- profiling or automated decision-making;
- data concerning vulnerable individuals, including tenants or service users;
- significant external sharing or supplier processing.

1.2 DPIAs are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. DPIAs are an integral part of data protection by design and by default.

1.3 A DPIA is a process which helps an organisation to identify and reduce the data protection risks of a project. An effective DPIA will be used throughout the development and implementation of a project, using existing project management processes. A DPIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

1.4 DPIAs are most effective when carried out for new projects, as they can help shape implementation and reduce data protection risks from the outset. They can also be used for changes to, or reviews of, existing systems where improvements can still be made. DPIAs identify and mitigate data protection risks early by assessing how personal data and technology will be used in practice, often with input from those involved in or affected by the project. They help address risks to individuals, such as harm or distress, and to

organisations, including financial and reputational damage from data breaches. Higher-risk and more intrusive projects generally have a greater privacy impact, and organisations should determine how best to assess and manage these risks.

2. Process

2.1 The DPIA process is a flexible one that can be integrated with an organisation's existing approach to managing projects. The time and resources dedicated to a DPIA should be scaled to fit the nature of the project.

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

2..3 A DPIA should incorporate the following steps:

a. Identifying the Need for a DPIA

- Use screening questions to assess potential privacy impacts.
- Consider privacy requirements during project planning.
- Engage stakeholders early to discuss data protection risks.
- Define project objectives and incorporate privacy considerations into project design.

b. Describing Information Flows

- Document how personal information will be collected, used, shared, stored, and retained.
- Identify potential unintended uses of data, such as function creep.
- Consult users and stakeholders on practical implications.
- Consider potential future uses of information.

c. Identifying Privacy and Related Risks

- Identify risks to individuals, including privacy intrusions and potential harm.
- Assess organisational risks, such as regulatory action, reputational damage, and loss of trust.
- Check compliance with data protection legislation.
- Record and assess the likelihood and impact of identified risks.

d. Identifying and Evaluating Privacy Solutions

- Develop measures to eliminate or reduce data protection risks.
- Evaluate the costs and benefits of mitigation options.
- Update and review the data protection risk register.
- Record any residual risks accepted by the organisation.

e. Signing Off and Recording DPIA Outcomes

- Obtain appropriate approval for the DPIA.
- Produce and maintain a DPIA report or summary.
- Consider sharing outcomes with relevant stakeholders.
- Ensure approvals are proportionate to the project's risk and scale.

f. Integrating DPIA Outcomes into the Project

- Implement agreed privacy controls and recommendations.
- Monitor and update the DPIA throughout the project lifecycle as needed.
- Record implementation actions.
- Refer to the DPIA when the project is reviewed, changed, or expanded.

g. Stakeholder Consultation

- Consult internal and external stakeholders throughout the process.
- Maintain a feedback mechanism to capture and address stakeholder views.

2.4 The Data Protection Lead must approve DPIAs where:

- special category data is involved;
- criminal offence data is involved;
- automated decisions may have significant effects;
- vulnerable individuals are affected;
- external suppliers process personal data;
- international transfers may occur;
- residual risk remains high after mitigation.

2.5 Where high residual risk remains and cannot be sufficiently mitigated, the Data Protection Lead must consider whether prior consultation with the ICO is required before processing begins.

Version History	
Procedure Name	Data Protection Impact Assessment Toolkit and Form
Lead Officer	Company Secretary (Data Protection Lead)
Date of Issue	August 2026
Review Date	August 2029
Regulation based on	UK General Data Protection Regulation (GDPR) and Data Protection Act 2018
Parent Policy	Group Data Protection Policy 2026
Version Code	2 Changes considering the Data (Use and Access) Act 2025

▪ Responsibility for entering into a contract remains with the relevant person with authority to do so even if you are asked to make DPIA checks ▪ Where any staff member is seeking to use organisations that share client or staff data, they should undertake research and be confident in the organisation prior to entering any agreement with them. ▪ Are you assured of the organisation and its integrity in how it uses personal data - include a link to the organisations Privacy Notice, how data is stored. ▪ Colleagues who are delegating to a colleague should still have accountability, check and sign off for assurance ▪ Will the new or contractor be a controller or a processor of data? Where the organisation is acting as a controller, a Data Sharing Agreement may be required. Where it is acting as a processor on ccha's instructions, appropriate processor terms, including Article 28 UK GDPR requirements, will be required. ▪ Lawful basis under Article 6 may be: consent (only where genuinely appropriate), performance of contract, legal obligation, the vital interests of the client, or legitimate interests ▪ Special Category Data: If special category data is processed, identify both the Article 6 lawful basis and the relevant Article 9 condition. Examples may include explicit consent, employment/social security obligations, vital interests, data manifestly made public, legal claims, substantial public interest, health or social care purposes, or public health reasons, where applicable.	▪ Who did you engage with at the organisation to find out about their use/potential use of data? ▪ Whose data is being shared, clients, staff. Do ccha's policies/privacy notices or processes permit you to collect the data and subsequently store it? ▪ What is going to happen with the data? - collection, storage, usage, disposal ▪ How much personal data will be handled (approx. number of subjects) ▪ Why do you need to use personal data in that way. ▪ Where it is staff or client data, do you need to obtain permissions, do you have that? ▪ Where it is **mandatory** for clients/staff to participate, you should not need to collect permissions, but you must be clear of your lawful basis for processing under Article 6 of the UK GDPR. ▪ Legitimate interests, if this is the only reason for collecting data you MUST complete a legitimate interest assessment and store with the completed and signed DPIA

Questions	**Answer**
❶ Name of the Organisation/Supplier, briefly what they do or will be doing for ccha	
❷ Main contact at the organisation/ and email	
❸ Will the project involve collection of new personal data? If yes, what data and who will collect it.	
❹ Will the project compel individuals to share information about themselves that we do not already have? (if yes, what information)	
❺ Will the personal data be shared with or be accessible by external organisations? (if yes, please specify what data and whose personal data will be shared)	
❻ Who will have access to the personal data within ccha/cchadl (please include details if there are several levels of access available)	

❼ Are you using (existing) information about individuals for a new purpose, or in a way it is not currently used? Do you have a lawful basis for that?	
❽ Does the project involve using new technology that might be perceived as being privacy intrusive? (if yes, please specify)	
❾ Will the project result in making decisions or taking actions about individuals in ways that can have significant impact on them (e.g. automated decision making).	
❿ Will the project result in the use of special category or sensitive information? (if yes, please specify)	
⓫ Will the project require you to contact individuals in ways they may find intrusive over and above existing policy and process?	
⓬ Will the processing of personal data take place outside the UK? (if yes, please provide details including what transfer mechanism or safeguard applies?)	
⓭ What security measures will be in place to protect personal data both internally and externally (if shared externally)?	
⓮ If the personal data will be shared with or be made accessible to external organisations, please specify the arrangement in place: controller-to-controller sharing possible DSA; processor arrangement: processor/data processing agreement; joint controller arrangement: joint controller arrangement. Use the ccha model DSA or the new supplier or contractor may provide one.	NB All DSAs must be read carefully prior to signing
⓯ Who will ensure that data is destroyed at the end of the contract? Staff and management responsible must agree who is responsible for the deletion of data when no longer required.	
Summarise: risks to individuals, likelihood and impact, mitigations, residual risk rating	
Risk owner	
Actions and due dates to further mitigate risks	
⓰ Provide Privacy Notice or Link to website	
⓱ Checked by: Print Name and include today's date / review date	
Data Protection Lead Approval and date (where required):	

Appendix 4: Data Breach Procedure

1. Introduction

1.1 ccha holds a large amount of personal data in hard and electronic copy. This includes personal data (names, addresses etc.) and special category data (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) about service users, residents and members of their household, employees of ccha, and other individuals.

1.2 In accordance with UK data protection legislation[1], ccha as the controller must take appropriate steps and have systems in place to safeguard the personal data and special category data it holds to ensure that it is not disclosed accidentally or deliberately, nor is it lost or stolen.

1.3 In the event that a personal data breach occurs, it is vital that appropriate steps are taken to minimise any associated risks.

1.4 Relationship with other policies and procedures

Other policies and procedures within ccha interface with the Data Breach Procedure, they include:

- Group Data Protection Policy
- Subject Access Request Procedure
- Data Protection Impact Assessment Procedure Toolkit and Form
- NHF Data Retention Schedule (adopted)
- cctv Procedure
- Privacy Notices

2.0 What is a breach?

2.1 The UK GDPR defines personal data breach as "…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."

2.2 Some examples of personal data breaches are:

- Loss, or theft of personal and special categories of personal data

[1] By this we mean the UK Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (as amended), and the Data (Use and Access) Act 2025 (DUAA).

- Loss, or theft of equipment on which data is stored
- Unauthorised access to data
- Unauthorised disclosure e.g. by a member of staff
- Human error such as disclosing, emailing, posting etc. personal data by mistake
- Failure of equipment and therefore data held on it
- Cyber-attack
- Where information is obtained by deception e.g. by deceiving a member of staff

3.0 How do I report a breach?

3.1 When a personal data breach occurs you should:

i. Immediately report it to your Line Manager, as the primary point of contact. Your report should:
   a) provide full and accurate details of the incident
   b) describe the type of data involved
   c) identify the affected individual(s).

ii. Where the breach occurs because of a crime e.g. theft of equipment on which personal data is stored, personal assault on staff, etc., this must be reported to the police, and the crime reference number should be included in the report.

iii. You or your Line Manager must notify the Company Secretary who is ccha's Data Protection Lead **within 24 hours of the breach occurring and seek support from IT where required**, by logging a report of the breach.

iv. If your Line Manager is not available, report directly to the Company Secretary or a member of Leadership.

4.0 What steps do I need to take to investigate a breach?

4.1 The lead officer responsible for investigating the personal data breach should instigate an investigation within 24 hours of the breach being discovered to assess whether it is notifiable to the Information Commissioner's Office.

4.2 During the investigation, the officer will summarise findings and report back considering the following: when the breach occurred;

- when ccha became aware of it;
- categories and approximate number of individuals affected;
- categories and approximate number of records affected;
- whether the breach has been contained;
- likely consequences;
- remedial steps taken or proposed.

4.3 The investigation will include a risk assessment to determine the actual and likely consequences of the breach and whether the affected individuals have suffered or are likely to suffer harm as a result. In particular, the investigation will assess the risk of ID fraud and/or potential financial loss to the affected individuals.

5.0 Containment and Recovery

5.1 The appropriate course of action to be taken to contain the breach will be agreed with the Data Protection Lead including any resourcing needed to limit the impact of the breach, if necessary.

6.0 Do I need to notify individual(s) or the ICO about a breach?

6.1 Affected individuals will be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms. Any notice should include a description in clear and plain language of the breach and the steps taken to mitigate the risks, plus advice on what steps the individuals should take to protect themselves. The notice should contain the following information and measures:

- Communicate the name and contact details of ccha's Data Protection Lead or other contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken by ccha to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Whether the ICO has been notified and what information was involved.

6.2 ccha is not required to notify individuals if any of the following conditions of Article 34 of the UK GDPR are met:

- Security measures were applied to the personal data affected by the personal data breach, which render the personal data unintelligible to any person who is not authorised to access it, such as encryption; or
- ccha has taken subsequent measures which ensure that the risk to affected individuals is no longer likely to materialise (e.g. remote wiping of devices); or
- it would involve disproportionate effort. In that case, ccha will send out a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

6.3 ccha's Data Protection Lead will assess whether the breach is likely to result in a risk to the rights and freedoms of individuals, the extent and seriousness of the breach and, where appropriate, seek legal advice, as to whether to inform the Information Commissioner's Office ('ICO').

6.4 Article 33 of the UK GDPR makes notifying a personal data breach to the ICO a mandatory requirement within 72 hours of the organisation becoming aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In practice, assessing this risk will be achieved via consideration of the matters outlined at 4.2 above.

6.5 Where it is decided that the breach is notifiable, this should be made to the ICO, without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where the notification to the ICO is not made within 72 hours, it must be accompanied by reasons for the delay.

7.0 How will we implement lessons learnt?

7.1 A review of the incident will be conducted by ccha's Data Protection Lead to identify areas of improvement.

7.2 Any recommended actions and changes to systems, policies and procedures and training will be documented and agreed with the Line Manager for implementation as soon as possible.

7.3 Details of all breaches, outcomes and actions will be reported to the next scheduled meeting of the Directors and subsequently to the Audit and Committee.

8.0 Do I need to keep a record of breaches?

8.1 In line with Article 33 of the UK GDPR ccha will keep a record of any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This documentation enables ccha, as well as the ICO, to verify compliance with the GDPR at any stage.

9.0 When will this procedure be reviewed?

9.1 This procedure will be reviewed every three years or following any relevant changes in law or guidance from the ICO.

9.2 We may carry out checks or audits from time to time to ensure that the requirements of this procedure are followed.

Version History	
Procedure Name	Data Breach Procedure
Lead Officer	Company Secretary (ccha's Data Protection Lead)
Date of Issue	August 2026
Review Date	Reviewed and updated in line with the Data (Use and Access) Act 2025 Review August 2029
Regulation based on	UK GDPR and Data Protection Act 2018
Parent Policy	Group Data Protection Reviewed August 2026
Version Code	2

Appendix 01e Data Retention Schedule

ccha have adopted the NHF Retention Schedule

This is a spreadsheet and available internally on the Hub, and available on request for customers.

Appendix 6: Closed Circuit Television (CCTV) Procedure

1 Introduction

1.1 Croydon Churches Housing Association Limited ("ccha") uses CCTV images to provide a safe and secure environment for staff, volunteers and visitors and to protect ccha's property.

1.2 This procedure sets out the accepted use and management of CCTV equipment and images to ensure ccha complies with UK data protection legislation[1], (UK GDPR) the Human Rights Act 1998 and other legislation (referred to together in this procedure as "the Legislation").

1.3 Where in this procedure there is reference to the Legislation this includes all statutory amendments and subordinate legislation and regulations.

1.4 ccha has produced this procedure in line with the Information Commissioner's guidance on surveillance (www.ico.org.uk) and has updated the procedure in light of the UK GDPR.

1.5 ccha has appointed the Company Secretary as its Data Protection Lead.

1.6 Other policies and procedures within ccha interface with the CCTV Procedure, they include: -

- Group Data Protection Policy
- Subject Access Request Procedure
- Data Breach Procedure
- Privacy Notice and Website Privacy Information
- Document Retention Procedure and (adopted) NHF Retention Schedule
- Data Protection Impact Assessment Toolkit and Form
- Departmental Compliance Statement
- Corporate Compliance Statement/Record of Processing Activities
- CCTV (recording and monitoring systems) Register

1.7 cccha reserves the right to use a third-party contractor to install and manage its ccha systems.

[1] ccha considers references to the UK GDPR in this Policy mean the UK GDPR as varied or supplemented by the Data Protection Act 2018 and all related legislation, whether in the policy or its appendices.

2 What Process Should We Follow When Installing CCTV?

2.1 Personal data processed by the CCTV system are images of employees, residents, service users, customers, the public in and around properties, premises and car parks.

2.2 The legal basis for the processing of personal data by the CCTV system is broadly for ccha's legitimate interests to prevent crime and anti-social behaviour on its premises. This is in line with Article 6(1) (f) UK GDPR. This purpose may be broadened to reflect specific circumstances as set out below.

2.3 Before installing a CCTV system, a data protection impact assessment (DPIA) must be carried out to identify the potential risks in relation to ccha's use of CCTV.

2.4 The DPIA should identify the purposes for installing the CCTV system, potentially including the following:

- Assist in prevention and detection of crime;
- Assist with the identification, apprehension and prosecution of offenders;
- Assist with the identification of actions that might result in disciplinary proceedings against staff and volunteers;
- Monitor security of ccha buildings and areas; and
- Create a safe environment.

As well as the benefits to be gained from use of the CCTV system, such as greater security for employees, service users, residents, customers and our property, including cash and goods. Once identified, the purpose for which the CCTV system is to be used must be recorded in writing on the CCTV register.

2.5 The DPIA must consider the effect and potential effects on the privacy of individuals having regard to the siting of the camera(s) and detail any mitigating steps which can be taken to avoid/lessen the risk of breach of data protection. Staff must seek the advice of ccha's Data Protection Lead when carrying out a Data Protection Impact Assessment.

3 What Should I Consider When Installing CCTV Equipment?

3.1 When installing CCTV, the equipment must be able to:

i. cover the area to be monitored and exclude areas that do not need to be monitored for the purposes set out in this procedure;

ii. produce clear images of a high quality, (i.e. of a standard that would be capable of having evidentiary value to the police);

iii. work effectively 24 hours per day, 7 days a week;

i. iv. have night-time monitoring;

ii. work effectively within normal indoor conditions;

iv. produce images of sufficient size, resolution and frames per second to meet the requirements of the purposes;

v. record in real time on a continuous basis.

3.2 All SMT managers, or those in an equivalent role, will be responsible for the management and operation of all CCTV systems operated by ccha within their departments.

3.3 ccha has a central register of all CCTV installations. Each new CCTV system must be included on the register. Annually, the Data Protection Lead will circulate details of the CCTV register to relevant managers for confirmation.

3.4 Occasionally, it may be necessary to undertake covert monitoring. We only undertake covert monitoring where there are strong grounds for suspecting criminal activity or equivalent malpractice. Covert monitoring will take place within a strict timeframe and will only be targeted at gaining evidence. This type of monitoring can only be authorised by the Chief Executive and after a Legitimate Interest form has been approved by them.

4 What Signage Should be displayed?

4.1 We are required to notify individuals if they are in an area where CCTV surveillance is being carried out. Typically, this is achieved using prominent signs which are located at the start of the CCTV zone, with reminder notices placed at various locations inside the monitored zone.

4.2 The signs should:

i. alert individuals that CCTV is in place;
ii. Signage should be clearly visible and readable. (the size of the sign will depend on the location and how visible it is to individuals);
iii. include the following information where this is not obvious:
    a) the identity of the organisation responsible for the system;
    b) a description of the purpose(s) of the system; and
    c) details of who to contact regarding the system

5 How Should We Store CCTV Imagery?

5.1 CCTV images must be stored securely and in a secure place (whether physically or in the cloud) to which access is controlled (this is particularly important where images may be used for evidentiary purposes). We have an obligation to keep CCTV images always secure to prevent unauthorised viewing or disclosure. To ensure that we meet our security obligations you must ensure that:

iii. access to the images is restricted to authorised staff only. If there is a need to access CCTV imagery, please contact ccha's Data Protection Lead.

iv. disclosure of images (where permitted) is undertaken using a secure method of transmission or delivery (to minimise the risk of images getting lost in transit or being intercepted);

v. CCTV storage systems where images are stored should be always kept secure.

vi. any images stored on a computer must be appropriately protected.

5.2 Images should be retained for no longer than the retention periods specified in this procedure.

6 How Should I Deal with A Request to View or Release CCTV

6.1 As a rule, CCTV images should only be viewed and accessed by authorised personnel. Other staff and third parties (such as the police) should only be allowed to view the images where it is necessary in connection with the purposes set out below or as otherwise permitted in this procedure.

6.2 The following rules apply to the viewing of CCTV images:

i. the viewing of live images on monitors should be restricted to an authorised operator of the CCTV system and appropriate ccha personnel;

ii. recorded images should be viewed in a restricted area (e.g. a designated secure office). Access to this area should be restricted whilst the viewing is taking place.

6.3 In certain circumstances it may be necessary to release the CCTV images to a third party, such as the police. The disclosure is likely to involve the physical delivery of the images or copies to the third party (e.g. by email). Disclosures to third parties must be consistent with the purposes set in this procedure. Any disclosure of images must be approved by the relevant manager following a

written request and approval of the Company Secretary who is the Data Protection Lead.

6.4 Disclosures are permitted post approval in the following circumstances:

i. Crime prevention or detection purposes - where the disclosure is requested for the purpose of preventing or detecting crime, apprehending or prosecuting offenders, or assessing or collecting tax (the crime and taxation purposes).

ii. Statutory or other legal obligation - the disclosure of the images may be required under statute (other than under the UK GDPR) or may otherwise be legally required (e.g. under a court order). In this situation:

a) we must disclose the CCTV images if the statutory provision imposes upon us a **mandatory** duty to disclose or a court order requires disclosure;

b) we can choose whether to disclose the CCTV images if the statutory provision imposes upon us a **discretion** as to whether to disclose; and

6.5 In limited circumstances it may also be possible to make a disclosure where it is necessary for the purpose of establishing, exercising or defending legal rights, obtaining legal advice or in connection with legal proceedings. This covers not just our legal rights but also those of third parties.

6.6 A record should be kept of all requests for disclosure of CCTV images, together with any reasons for refusing a request. If a disclosure is approved and CCTV images are disclosed to a third party, a record should be made of the following:

i. the date the written request was received

ii. the date and time of the disclosure;

iii. the name of the person to whom the disclosure is made and the organisation he or she represents;

iv. the reason for the disclosure and the images disclosed;

vii. the basis upon which the disclosure was made (under UK GDPR);

viii. the location where the images are to be kept;

v. the outcome, if any, of the disclosure;

vi. the date and time the images were returned (if applicable); and

ix. if the disclosure is to the police, record any crime incident number to which the images relate and ask the collecting police officer to sign for the images when they are handed over.

6.7 Where a decision has been made to disclose CCTV images, the disclosure must be made securely so that the images are received by the intended recipient. For example, where a wireless transmission system is used to disclose the images, sufficient safeguards must be put in place to protect the transmission from being intercepted in transit (e.g. encryption).

7 How long should we keep CCTV Records

7.1 CCTV images held on the hard drive of a PC or server will be overwritten on a recycling basis once the drive is full, and in any event will not be held for more than 30 days except where they need to be retained longer for evidential purposes.

7.2 In such cases, the images will be stored appropriately and will be held securely by ccha's Data Protection Lead, Middle Managers or equivalent role until such time as handed over to the police or other authorised body.

7.3 ccha's IT policies do not support the use of removable media such as CDs and should not be used unless specifically authorised by the Data Protection Lead. In such cases, managers are responsible for ensuring that any images stored on any removable media are disposed of securely once the purpose of the recording is no longer relevant.

8 How do I manage a Subject Access Request to view CCTV

8.1 The UK GDPR gives individuals (data subjects) the right to access personal data about themselves, including CCTV images.

8.2 All requests for access to images by data subjects (when they are asking for access to images of themselves) should ideally be made in writing to ccha for the attention of ccha's Data Protection Lead and will be managed in line with the Subject Access Request procedure. However, requests can be made in any form, including verbally.

8.3 The manager responsible for the system will liaise with the Data Protection Lead to determine whether disclosure of the images will reveal third-party information.

8.4 Requests for access to CCTV images must include sufficient information to enable ccha to identify:

i. The date and time when the images were recorded

ii. The location of the CCTV camera

iii. Proof of identity and a description of the data subject

8.5 Decisions regarding the disclosure of data following a request from a data subject will be made and communicated to the requester in accordance with ccha's Group Data Protection Policy and Subject Access Request Procedure.

9. How do I deal with a resident's request to install domestic cctv systems?

9.1 Residents **must** ask our permission before installing CCTV systems including video doorbells because we must be sure that the system does not contravene UK data protection legislation, negatively impact the privacy rights of neighbours and other residents or cause damage to property. Generally, we will be happy to grant permission providing the following criteria are met:

i. The system covers images of the resident's property only

ii. Any monitoring systems cannot cover communal areas

iii. Suitable clear signage is installed by the resident.

iv. Reasons for the monitoring systems are provided

v. That the system complies with UK Law

9.2 Residents are responsible for the images they record and must ensure they are complying with legislation and adhering to the guidance. Failure to do so is a breach of their contract. More information can be found at Surveillance Cameras Commissioners website.

10 Periodic Review

10.1 The relevant manager will carry out a periodic review of the continued justification for and effectiveness of the CCTV system in operation within our business in fulfilling the purposes set out in this procedure and of general compliance with this procedure.

10.2 We may carry out checks or audits from time to time to ensure that the requirements of this procedure are being followed.

11 Further Information

11.1 Complaints and enquiries about the operation of ccha's CCTV systems can be submitted to ccha for the attention of the Data Protection Lead contact

details: customers@ccha.biz Complaint details are covered in Appendix 7.

Version History	
Procedure Name	CCTV Policy part of ccha Group Data Protection Policy
Lead Officer	Company Secretary (Data Protection Lead)
Date of Issue	August 2026
Review Date	Updated June- August July 2026 in line with the Data Use and Access Act (DUAA) Review August 2029
Regulation based on	UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
Parent Policy	Group Data Protection Policy 2026
Version Code	2

Appendix 7: Procedure for Complaints Relating to Individual Rights Requests (UK GDPR)

1. Purpose and Scope

ccha is committed to ensuring that individuals can exercise their rights under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, and can raise complaints where they believe ccha has not handled their personal information in accordance with data protection law. These rights and complaints include, but are not limited to, the right of access (Subject Access Requests), rectification, erasure, restriction of processing, data portability, objection to processing, rights relating to automated decision-making, concerns about the collection or use of personal data, the security of personal data, and complaints arising from an actual or suspected personal data breach.

2. Raising a Complaint

If an individual is dissatisfied with the way the organisation has handled a request to exercise their data protection rights, or believes that ccha has otherwise failed to comply with data protection law, they may submit a complaint to the organisation. This includes complaints relating to actual or suspected personal data breaches, concerns that personal data has not been kept secure, or concerns about how personal data has been collected, used, shared, retained, amended or deleted. Complaints should be made in writing where possible and should include sufficient information to enable the organisation to investigate the matter.

2.1 Complaints may relate to any UK GDPR or Data Protection Act 2018 matter, including:

- The organisation's response to a Subject Access Request (SAR);
- Alleged delays in responding to an individual rights request;
- A decision to refuse a request in whole or in part;
- The adequacy of information provided in response to a request;
- An actual or suspected personal data breach, including loss, theft, unauthorised disclosure of, unauthorised access to, alteration of, or accidental or unlawful destruction of personal data;
- Concerns that personal data has not been kept secure or confidential;
- Concerns about how personal data has been collected, used, shared, stored, retained or deleted;
- Concerns about transparency, fairness, lawful basis, consent, direct marketing, profiling or automated decision-making; or
- Any other concern regarding the handling of an individual's personal data or data protection rights.

3. Handling of Complaints (First Stage)

Upon receipt of a data protection complaint, ccha will:

1. Acknowledge receipt of the complaint without undue delay.
2. Review the circumstances of the original request and the response provided.
3. Consider whether the request was handled in compliance with applicable data protection legislation, internal policies, and regulatory guidance.
4. Provide a written outcome to the complainant, including any corrective action identified without undue delay and within 30 days.
5. Maintain records of complaints and their resolution for audit and accountability purposes.

Where a complaint relates to an actual or suspected personal data breach, ccha will also consider whether the matter must be managed under its personal data breach procedure, including assessment of risk to individuals, notification to the ICO within the required timeframe where applicable, communication with affected individuals where required, and recording of the breach and decisions taken.

4. Outcomes

Following investigation, the ccha may:

- Uphold the original decision;
- Provide additional information or explanation;
- Amend or supplement a previous response;
- Take corrective action to address any identified procedural shortcomings; or
- Where appropriate, apologise and implement measures to prevent recurrence.

5. Escalation to the Information Commissioner's Office (ICO) (Second Stage)

If an individual remains dissatisfied following the organisation's internal review, they have the right to raise their concerns with the Information Commissioner's Office (ICO), the UK's independent supervisory authority for data protection matters. The ICO can be contacted via: **Information Commissioner's Office,** Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone: 0303 123 1113 Website: www.ico.org.uk

Version History	
Procedure Name	Procedure for Complaints Relating to Individual Rights Requests (UK GDPR)
Lead Officer	Company Secretary (named Data Protection Lead
Date of Issue	August 2026
Review Date	August 2029
Regulation based on	General Data Protection Regulation (UK GDPR) and Data (Use and Access) Act 2025 (DUAA)
Parent Policy	Group Data Protection Policy 2026
Version Code	1

Appendix 8 Group Data Protection Policy Glossary of Terms

Biometric Data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images.

Conditions for Processing: ccha are only permitted to process personal data where we have identified a legal right to do so,

Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Controller: ccha will determine the purposes for which data is collected and the way it is processed. ccha is the data controller for data we choose to process, but we may also act as or engage a Data Processor *see below*.

Data Privacy Impact Assessment: A process designed to help organisations identify and mitigate privacy risks associated with proposed data processing activities. For further information, see ccha's Privacy Impact Assessment guidance.

Data Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Processing: Any operation or set of operations performed upon personal data, be it by electronic systems or not. e.g.: collection, storing, altering, retrieving, using, disclosing by transmission, restricting, erasure or destruction.

Data Protection by Design and Default: Requires us to think about data protection and privacy from the very offset of anything we plan to do with people's data, for example when procuring or designing new tools for managing data and embarking on new uses for data. This is particularly the case when any new initiative, project, or data hosting tool could pose a high risk to privacy or data security. The named Data Protection contact must be involved in cases where this applies.

Data Subject: A natural person (staff, student or third-party) whose data is being processed.

Genetic Data: Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Identifiable Natural Person: A person 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.

Integrity and Confidentiality: The use of appropriate technical and organisational security measures to protect personal data.

Named Data Protection Contact: A representative for ccha who oversees GDPR compliance, handles Subject Access Requests and complaints, communicates with the Information Commissioners office and as the data-privacy expert for ccha, provides advice on all aspects of GDPR.

Personal Data: Any information relating to data subject that can identify them either directly or indirectly.

Personal Data Breach: The accidental or unlawful destruction, loss, alteration, or disclosure of personal data. In the event of a breach of data that could have serious consequences for those whose data has been compromised, it must be reported to the ICO within 72 hours. A breach may result in severe brand damage through loss of trust, or even a fine of up to €20 million or 4% of global turnover - whichever is greater. Failure to evidence appropriate controls could lead to a fine of up to €10 million or 4% of global turnover.

Principles: The fundamental principles imbedded within the GDPR which set out the main responsibilities for organisations. These are:

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Restriction on Processing: The marking of stored personal data with the aim of limiting their processing in the future.

Right of Access: Entitles the data subjects to have access to and information about the personal data being processed by the data controller.

Special Categories of Data: Data concerning the racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, or data concerning health or sex life or sexual orientation of an individual.

Subject Access Requests: Requests from Data Subjects to receive a copy of data held about them.