Data protection policy

Author: Head of ICT & Business Intelligence

Version 1.2

March 2023

Glossary

Controller

A controller determines the purposes and means of processing personal data.

Data Processing

This refers to all collection, use, sharing and deletion of personal data.

Data Protection Act 2018

The Data Protection Act 2018 updates the original Act of 1998, complementing (and diverging from) the GDPR.

Data Protection Leads

The strategic lead for data protection is the appointed member of the Corporate Management Team; the operational lead is the acting Data Officer

DPO

The Data Protection Officer is a statutory role responsible for overseeing data protection strategy and implementation to ensure compliance with the requirements of the GDPR and other relevant data protection legislation. CBH is considered to be a public authority and must have a DPO. CBH and CCC currently have a joint DPO.

Data Subject

The person about whom data is held.

Data Subject Access Request

A request for personal information, usually made by the Data Subject to whom it relates.

GDPR

UK General Data Protection Regularion governing the collection and processing of personal data and including changes to data subjects' rights.

ICO

The Information Commissioner's Office is the statutory regulator.

Information Asset Owner

The person responsible for managing the risks to personal information and business critical information held within a department.

Information Asset Register

A mechanism for understanding and managing an organisation's assets and associated risks.

Personal Data

Personal data is defined as data relating to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller. This will include any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processor

A processor is responsible for processing personal data on behalf of a controller.

Senior Information Risk Owner

The SIRO has overall responsibility for managing the risks to personal information and business critical information for the organisation.

Special category data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data or biometric data for the purpose of uniquely identifying an individual; data concerning health or data concerning an individual's sex life or sexual orientation.

Contents

1. Introduction & purpose

Colchester Borough Homes (CBH) is a limited company set up, and wholly owned by, Colchester City Council (CCC). CBH operates on behalf of CCC. The two organisations collaborate closely on data protection to ensure that all personal data is handled lawfully and correctly.

CBH needs to collect and use information about the people with whom it works; members of the public; current, past and prospective employees; customers; suppliers and others in order to carry out its duties. This Data Protection Policy sets out the organisation's commitment and approach to data protection and provides a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance.

The processing of personal data in the United Kingdom is regulated by law. The principle statutory instrument setting out the legal obligations of those handling personal data is the Data Protection Act 2018 (DPA 2018). Other laws inter-relate with the DPA 2018 including, but not limited to, the UK General Data Protection Regulation (GDPR), the Privacy and Electronic Communications Regulations (2003) and the Freedom of Information Act (2000). These laws are collectively referred to in this Policy as Data Protection Legislation.

2. Application of policy

CBH is committed to compliance with all relevant Data Protection Legislation and will formally delegate appropriate powers and responsibilities to its personnel to ensure that it is fully able to comply with Data Protection Legislation and its own defined standards in the field of data protection and information governance.

CBH will ensure that sufficient and appropriate resources are available to ensure that it meets both its legal obligations in respect of Data Protection Legislation and the standards that it sets through its policies. CBH will ensure that the organisation works within the 6 data protection principles and that it will implement sufficient controls to ensure that it is able to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and decisions relating to data processing activities.

CBH will uphold the rights and freedoms of people conferred on them by the Data Protection Legislation. It will ensure that those rights and freedoms are appropriately taken into account in the decisions it takes which may affect people and will ensure that it has sufficient controls in place to assist people who wish to exercise their rights. CBH will ensure that data subjects have appropriate access, upon written request, to personal information relating to them and will ensure the data subjects' rights to rectification, erasure, restriction, portability and object are adhered to.

This policy applies to all CBH activities and operations which involve the processing of personal data. This policy applies to anyone who is engaged to process personal data for or on behalf of CBH including: employees, volunteers, casual and temporary staff, directors and officers, Board members, Councillors and third-parties such as sub-contractors and suppliers, and anyone who CBH shares or discloses personal data with/to.

CBH will ensure that all personal data is handled properly and with confidentiality, at all times, irrespective of whether it is held on paper or by electronic means. This includes the:

- Obtaining of personal data
- Storage and security of personal data
- Use and processing of personal data
- Disposal of or destruction of personal data..

3. The principles of data protection

Whenever collecting or handling information about people CBH will ensure that:

- Personal data is processed, lawfully, fairly and in a transparent manner
- No data collection or processing activities will be undertaken or commissioned without an appropriate privacy notice being provided to the person about whom data are being collected
- No data collection or processing activities will be undertaken or commissioned without there being a lawful ground for the data processing activities intended to be applied to the personal data
- The purposes for which personal data is obtained and processed are specified and that data is not used for any other purpose (unless permitted within the legislation).
- Processing of personal data is adequate relevant and limited to what is necessary
- It uses reasonable endeavours to maintain data as accurate and up-to-date as possible
- Personal data is retained only for as long as necessary
- CBH will maintain a data retention schedule setting out approved retention periods
- Data is disposed of properly
- All personal data is processed in accordance with the rights of the individual concerned
- Personal data is processed in an appropriate manner to maintain security
- The movement of personal data is done in a lawful way, both inside and outside CBH, and that suitable safeguards exist, at all times.
- A data breach reporting procedure is maintained
- All employees and those with access to personal data are aware of it
- CBH will log all personal data breaches and will investigate each incident without delay

- Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach
- If a breach is assessed as meeting the threshold for reporting to the Information Commissioner's Office, a report will be made without delay
- It strives to foster a culture of data protection by design and by default in all data processing activities

4. Roles and responsibilities

4.1 Roles

- The Data Protection Officer (DPO) is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements
- The Strategic Lead for data protection is appointed from the Corporate Management Team and is responsible for data protection strategy and planning.
- The Operational Lead for data protection (acting data officer) is the first point of contact for CBH staff and members of the public in data protection matters. The role includes processing data and information requests, and working with staff and the DPO to help ensure and monitor compliance.
- The Senior Information Risk Owner has overall responsibility for managing the risks to personal information and business critical information for the organisation.
- Information Asset Owners have responsibility for managing the risks to personal information and business critical information held within a department.
- The CBH Board will have a regular opportunity to oversee data protection compliance management on the principal advice of the Chief Executive Officer.

4.2 Responsibilities

The Chief Executive Officer is the Accountable Officer ultimately responsible for ensuring that all information is appropriately protected.

CBH will ensure that:

- A member of staff, the Data Protection Officer (DPO), is appointed who has specific responsibility for data protection within CBH
- Any disclosure of personal data is in compliance with the legislationand with approved procedures
- Anyone managing and handling personal information understands that they are legally bound to follow good data protection practice
- Anyone managing and handling personal information is appropriately trained and supervised

- Staff have access only to personal information relevant to their roles
- Appropriate advice and guidance is available to anyone wanting to make enquiries about personal information held by CBH
- Enquiries and requests regarding personal information are handled courteously and within the time limits set out in law
- All staff and Board members are fully aware of this policy and of their duties and responsibilities under Data Protection Legislation
- Where personal data may need to be shared with third parties in order to deliver services or perform our duties, CBH will only share personal data when a lawful basis from the legislation can justify that sharing, where it is necessary to achieve a clear purpose and, with that purpose in mind, it is fair and proportionate to do so
- Data Protection Impact Assessments (DPIA) are conducted, and signed off by the Data Protection Officer
- A record of personal data processing is kept and maintained.

Everyone will ensure that:

- All data processing operations under their control or sphere of responsibility or commissioned by them are undertaken in compliance with this policy, related policies and data protection legislation
- Paper files and other records or documents containing personal and or special category data are kept securely and destroyed securely
- Personal data held electronically is protected by the use of secure passwords, is kept securely and destroyed securely
- All users must choose passwords which meet the security criteria specified by the Council
- Staff working remotely from home or elsewhere must keep any CBH-issued equipment they use secure, and prevent systems and data for which CBH is responsible being used or seen by members of their family or any other unauthorised person
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- Personal data is not stored on personal devices or forwarded to personal email accounts
- Personal data is not to be left where it can be accessed by persons not authorised to see it
- Personal data is kept up to date and accurate
- Personal data is kept in accordance with CBH’s retention schedule
- Any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support the Data Protection Officer in investigating and resolving breaches
- Where there is uncertainty around a data protection matter advice is sought from the Data Protection Officer
- appropriate disciplinary action will be taken Against staff held responsible for repeated personal data breaches.

CBH reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business

efficiency and effectiveness. No third-party data processors will be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation.

The joint CBH/CCC Data Protection Officer is responsible for:

- Advising CBH and its staff of its obligations under Data Protection legislation
- Overseeing the provision of Data Protection training, for staff within CBH
- The development of best practice guidelines
- Ensuring compliance checks are undertaken to ensure adherence with Data Protection Legislation
- Providing advice where requested on Data Protection Impact Assessments
- Cooperating with and acting as the contact point for the Information Commissioner's Office (ICO)
- Ensure that all personal data breaches are addressed and monitored, and report serious breaches to the Information Commissioner as well as to the CEO.
- Keep the organisation's Information Asset Register under review.

The Senior Information Risk Owner is responsible for:

- Ensuring that staff are aware of this policy
- Ensuring appropriate mechanisms are in place to support service delivery and continuity
- Being the organisation's leader and Champion for Information Risk Management and Assurance
- Advocating good information management and security practices
- Challenging risk mitigation
- Ensuring others are undertaking risk assessments and assurance activities
- Reporting annually to the Accountable Officer
- Being the senior manager with accountability for data protection and information risk and providing a link to CBH's Corporate Management Team (CMT).

Managers will ensure that:

- Information Asset Owners and Administrators help to maintain our Information Asset Register.
- Paper files and other records or documents containing special category data will be retained for the correct period and disposed of securely.
- All staff and Board Members are aware of their responsibilities under the GDPR and the Data Protection Act 2018 and complete Data Protection training.
- Staff working remotely from home or elsewhere are aware of the need to keep any company-owned equipment they use secure and prevent

systems and data for which we are responsible being seen or used by any unauthorised person.
- Agreements and contracts provide appropriate wording around data handling including, where relevant, specific responsibilities in respect of data processing.

All staff and Board members will ensure that they:

- Complete the data protection training provided.
- Understand their responsibilities under the jet protection legislationand the practical implications for their role.
- Observe principles of confidentiality, ensuring that information relating to staff, customers or others is not shared or discussed outside the organisation.
- Are familiar with the Data Subject Access Request procedure in order to advise and assist members of the public who wish to make a request.
- Promptly forward to the Data Officer any Data Subject Access Requests
- Report all breaches of personal data via the Breach Report App as soon as possible, and in all cases within 6 hours.

Our contractors, consultants, partners or other agents must:

- Confirm in writing that they will abide by the requirements of the data protection legislation with regard to information obtained from us.
- When requested, allow us to audit the protection of data held on our behalf.
- Ensure that they and all persons appointed by them who have access to personal data held or processed for or on our behalf are aware of this policy and are fully trained in their duties and responsibilities under the GDPR and Data Protection Act 2018.
- Indemnify us without limitation against any prosecutions, claims, proceedings, actions or payments of compensation or damages arising from their loss or misuse of data.
- Any breach of any provision of current data protection legislation by a contractor, supplier, partner agency or any of our data processors will be deemed as being a breach of any contract between us and that individual, company, partner or firm.

5. The Information Commissioner

Colchester Borough Homes and Colchester City Council are registered with The Information Commissioner as a data controller. The Data Protection Act 2018 requires every data controller who is processing personal data to notify and renew their notification on an annual basis.

6. References

- General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Privacy and Electronic Communications Regulations (PECR)
- Information Commissioner's Office website: www.ico.gov.uk.

7. Related documents

This policy should be read in conjunction with the following documents:

- Processing of special category and criminal convictions data policy
- Retention policy
- Information security policy
- ICT Acceptable use policy
- CCC ICT and data protection policies and standards
- Board Member code of conduct
- Staff code of conduct.

Document control sheet

Title

CBH Data protection policy - March 2023

File location

https://colchbh.sharepoint.com/sites/fnc/corpdoc/PolDevLib/CBH Data protection policy.docx

Consultation

CBH Information Governance Officer

CBH ICT Manager

CBH Corporate Management Team

Finance & Audit Committee

Approved

Board 01/03/2023

Next review 01/03/2024

Circulation method Website, email, SharePoint

Equality Impact Assessment

Required Yes

Latest 01/07/2020

Review due 01/04/2024

Equality Impact Assessment - Data Protection Policy .doc

Document amendment history

1.0 New September 2020

New policy based on CCC policy. Replaces Information & Confidentiality policy

1.1 Minor amends March 2022

Incorporating amendments to CCC policy approved December 2021.

1.2 Minor amends March 2023

Incorporating amendments to CCC policy during 2022 annual review.