Data protection policy

Author: Andrew Harley, Business Partner (acting data officer)
Angelique Ryan, Head of HR & Governance

Version 1.0

September 2020

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 CBC 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	The General Data Protection Regulation/Regulation (EU) 2016/679 - in force from 25 May 2018 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.
Sensitive Personal 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 Borough Council (CBC). CBH operates on behalf of CBC. The two organisations collaborate closely on data protection to ensure that all personal data is handled lawfully and correctly.

At CBH we collect a variety of information including personal, operational and commercial data. Under data protection legislation we act both as controller and as processor of personal data.

This policy outlines the guiding principles and key arrangements for the management of personal data. This includes data on our current, past and prospective employees, our tenants, leaseholders and other customers, and also on our suppliers, contractors, partners and others.

2. Application of policy

We fully endorse and adhere to the principles set out in data protection legislation (Data Protection Act 2018 and General Data Protection Regulations) and other legislation related to personal data. We will therefore ensure that all employees, Board members, contractors, agents, consultants, partners or anyone else who has access to any personal data held by or for us are fully aware of and abide by their duties and responsibilities under the relevant legislatory framework.

This policy and the procedures associated with it are reviewed annually to ensure that we continue to comply with all relevant statutory requirements.

We will ensure that all personal data is handled properly and with confidentially at all times, irrespective of whether it is held on paper or by electronic means.

This includes:

- the obtaining of personal data
- the storage and security of personal data
- the use and processing of personal data
- the disposal of or destruction of personal data.

We will comply with the Freedom of Information Act. We will also ensure that we meet all our responsibilities in respect of data subjects' rights, including those relating to access, rectification, erasure, restriction, and the right to object.

3. The principles of data protection

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

- personal data is processed, lawfully, fairly and in a transparent manner
- the purposes for which personal data is obtained and processed are specified and that data is not used for any other purpose
- processing of personal data is adequate relevant and limited to what is necessary
- any data used or kept is accurate and up to date
- personal data is retained only for as long as necessary
- 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 the Council, and that suitable safeguards exist at all times.

It should be noted that the verbal sharing or disclosure of information (in respect of staff, customers or others) may amount to the unlawful processing of personal data, and is fully subject to data protection principles and controls.

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 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

CBH will ensure that:

- Personal data held electronically is protected by the use of secure passwords, which are changed regularly.
- All staff and Board Members follow the data security policies of Colchester Borough Council, as required under the Management Agreement.
- A member of staff is appointed who has specific responsibility for day-to-day data protection issues.
- A Data Protection Officer is appointed who has a duty to advise CBH on data protection issues with a direct reporting line to the most senior officer, and with the operational independence to pursue their brief.
- Any disclosure of personal data is in compliance with the law and with approved procedures.
- All breaches of data security will be assessed and either recorded internally or reported to the ICO in accordance with the requirements of the legislation.
- Anyone managing and handling personal information understands that they are legally bound to follow good data protection practice.
- All staff are appropriately trained and supervised in managing and handling personal information.
- Appropriate advice and guidance is available to anyone wanting to make enquiries about personal information held by us.
- Enquiries and requests regarding personal information are handled courteously, within the time limits set by the GDPR and according to our Subject Access Procedure.
- All Board Members are made aware of this policy and of their duties and responsibilities under the law.
- Where it is necessary to share data with outside organisations, this is done under a written agreement setting out what is to be shared, how it is to be kept secure and committing the recipient to upholding the GDPR and current Data Protection Act with regard to the data shared with them. CBH will follow the statutory guidance issued by the ICO regarding data sharing. This guidance is available via the ICO's website www.ico.org.uk.
- New contracts are always examined as to whether they involve disclosures of personal data to other companies and information redacted as appropriate.
- All breaches of this policy will be investigated and dealt with in accordance with our disciplinary policies and procedures.

Managers will ensure that:

- Information Asset Owners help to maintain our Information Asset Register.
- Paper files and other records or documents containing personal and/or sensitive 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 will ensure that they:

- Complete the data protection training provided.
- Understand their responsibilities under the GDPR and Data Protection Act 2018 and 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 GDPR and Data Protection Act 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.

Where any of the above responsibilities have not been met, The Data Protection Officer (DPO) will:

- Monitor CBH's compliance with data protection legislation
- Develop best practice guidelines
- Ensure that all personal data breaches are addressed and monitored, and report serious breaches to the Information Commissioner as well as to the CEO.
- Ensure reviews of this policy and the practices and procedures pertaining to it to ensure continuing compliance with all relevant statutory provisions
- Review the organisation's Information Asset Register on an annual basis.

5. The Information Commissioner

The Data Protection Act 2018 requires every data controller who is processing personal data to notify and renew their notification on an annual basis..Colchester Borough Council and Colchester Borough Homes comply with this requirement through registration with The Information Commissioner as a Data Controller.

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:

- Information security policy
- ICT Acceptable use policy
- CBC ICT policies and standards
- Board Member code of conduct
- Staff code of conduct.

Document control sheet

Title	CBH Data protection policy – September 2020					
File location	https://colchbh.sharepoint.com/sites/fnc/corpdoc/PolDevLib/CBH Data protection policy.docx					
Consultation	CBC/ CBH Data Protection Officer - July 2020 CBH CMT – July 2020 Finance & Audit Committee - July 2020					
Approved	Board 01/09/2020					
Next review	01/09/2021					
Circulation method	Website, email, SharePoint					
Equality Impact Assessment	**Required**	Yes	**Latest**	21/07/2020	**Review due**	21/07/2021
	Equality Impact Assessment - Data Protection Policy .doc					

Document amendment history

Version	Type	Date	Notes
1.0	New	September 2020	New policy based on CBC policy. Replaces Information & Confidentiality policy