# Data Protection Policy

## 1. Purpose

1.1 Connexus is committed to protecting people's privacy, building trust, and using personal data responsibly.

1.2 This policy explains how we look after personal data, what colleagues must do, and where to find further guidance.

1.3 The policy supports our legal duties under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA2018), the Data (Use and Access) Act (DUAA) and the Privacy and Electronic Communications Regulations (PECR).

1.4 This is a high-level policy. Day-to-day requirements are set out in supporting procedures.

## 2. Scope

2.1 This policy applies to:

- All colleagues (permanent, temporary and agency)
- Board members
- All subsidiaries of Connexus Homes Limited
- Contractors, consultants and partners who handle data on our behalf

2.2 Everyone working for or with Connexus is responsible for following this policy.

## 3. Definitions

The following definitions are used in this policy: -

3.1 **Data Subject** – The individual whose personal information is being held or processed. A data subject is described as "any living/natural individual who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity."

Please note a deceased person does not have rights under data protection, but their data should still be treated confidentially.

3.2 **Personal Information/Data** – Information about living/natural individuals that enables them to be identified (directly or indirectly) e.g., name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual applicants, tenants, customers, service users, employees or board members of Connexus.

3.3 **Special Category Data** – Information about individuals which is more sensitive and, according to the relevant law and regulations, needs more protection. The categories are information about:
Racial or ethnic origin;
Political opinions
Religious or philosophical beliefs;
Trade union membership;
Genetic data;
Biometric data;
Health;
Sex life; and
Sexual orientation.

3.4 **Data Processing** – Includes obtaining, recording, holding, viewing, disclosing and disposing of data.

3.5 **Data Controller** – Is defined as a person, company, or other body that determines the purpose and means of personal data processing (this can be determined alone, or jointly with another person/company/body).

To be clear the Data Controller is Connexus Homes Limited or one of the subsidiaries "Connexus" and is not a named Officer of the Company.

For the official GDPR definition of "data controller," please see Article 4.7 of the UK-GDPR. For most purposes Connexus is the Data Controller and the Data Processor, however there may be circumstances where Connexus uses an external data processor.

3.6 **Data Processor** – Is defined as any person, company or other body who processes the data on behalf of the data controller.

3.7 **Explicit Consent** – Freely given and informed consent by the data subject to the processing of personal data about him/her.

3.8 **Lawful Basis** – The basis (as listed in the UK-GDPR) on which the data can be processed. These are:
Consent
Contract
Legal obligation
Vital interests
Public task
Legitimate interests

NB all of the above have specific meanings which are spelled out in the DPA 2018 and UK-GDPR, and on which guidance is provided by the ICO.

3.9 The main lawful basis for processing personal data that Connexus uses are: -

- Article 6.1(b) - Contract: the processing is necessary for a contract Connexus has with the individual, or because they have asked you to take specific steps before entering into a contract; or
- Article 6.1(e) – Public task: necessary to carry out a task in the public interest or in the exercise of official authority, with a clear basis in law.
- Article 9.2(g) – Substantial public interest: necessary for reasons of substantial public interest; or
- Article 9.2(h) – Health or social care: necessary for health or social care purposes or management of care systems or services.

3.10 **Director** – For the purposes of this policy, the word director(s) refers to executive directors rather than board members (non-executive directors).

3.11 **Colleague** – Includes paid employees, board and committee members (including 'co-optees').

## 4. What is Personal Data

4.1 Personal data is any information that can identify a living person, either directly or indirectly. This includes, for example:

- names and contact details
- tenancy and housing information
- financial details
- health or support needs
- photographs, CCTV images, and recordings

4.2 Some information, such as health data, ethnicity or safeguarding information, is more sensitive (special category data) and must be handled with extra care.

## 5. Our Data Protection Principles

6.1 Connexus follows the data protection principles set out in UK GDPR and DPA 2018. This means we will:

- Be fair and transparent – explain clearly how and why we use personal data
- Use data for specific purposes – and not reuse it inappropriately
- Only collect what we need – no excessive or unnecessary data
- Keep data accurate and up to date
- Keep data secure – protecting it from loss, misuse or unauthorised access
- Keep data only as long as needed – and dispose of it safely
- Be accountable – able to show that we comply with the law

## 6. Roles and Responsibilities

7.1 All colleagues must:

- handle personal data safely and respectfully
- follow Connexus policies and procedures
- complete required data protection training
- report any data protection concerns or breaches immediately

7.2 Managers must:

- promote good data protection practices
- ensure staff and contractors follow this policy
- make sure local processes are compliant

7.3 Data Protection Officer (DPO)
The DPO provides independent advice, oversight and assurance on data protection matters.

## 7. Collecting and Using Personal Data

7.1 Connexus will always be clear about:

- what data we collect
- why we need it
- how it will be used
- who it may be shared with

7.2 We will only process personal data where there is a lawful basis, such as:

- delivering a contract or service
- meeting a legal or regulatory duty
- protecting someone's vital interests
- carrying out a task in the public interest
- legitimate organisational purposes

7.3 Further detail is set out in the Lawful Basis Guidance.

## 8. Sharing Personal Data

9.1 We only share personal data where it is:

- lawful
- necessary
- proportionate

9.2 Appropriate safeguards and agreements must be in place when data is shared with third parties.

9.3 In limited circumstances, information may be shared to prevent harm or protect individuals. These situations are covered in the Data Sharing Procedure.

## 9. Data Security

9.1 Connexus uses appropriate technical and organisational measures to protect data, including:

- secure IT systems

- access controls
- encryption where appropriate

9.2 Colleagues must follow related policies, including:

- Information andrity Security Policy
- Hybrid Working Policy and Procedure
- Information Classification and Handling Guidance

## 10. Data Breaches

10.1 A data breach includes any loss, unauthorised access, disclosure or misuse of personal data.

10.2 All actual or suspected breaches must be reported immediately in line with the Data Protection Breach Procedure.

10.3 The DPO will assess breaches and manage any reporting to the Information Commissioner's Office (ICO) where required.

## 11. Retention and Disposal

11.1 Personal data is kept only for as long as it is needed for its purpose and in line with the Connexus Data and Document Retention Schedule.

11.2 When data is no longer required, it will be disposed of securely and safely.

## 12. Individual Rights

12.1 People whose data we hold have rights, including the right to:

- be informed
- access their data
- have inaccurate data corrected
- request deletion in certain circumstances
- restrict or object to processing
- data portability
- protections around automated decision-making

12.2 Requests are handled in line with the Data Subject Rights Request Procedure.

12.3 Individuals may also raise concerns or complaints about how their personal data is used, which will be handled in line with Connexus' Data Protection Complaints Procedure.

## 13. Transparency and Privacy Information

13.1 Connexus provides clear privacy information through:

- Privacy Notices
- tenant and customer communications
- our website

13.2 This explains what data we use, why we use it, and how individuals can exercise their rights.

## 14. Legal and Regulatory Requirements

14.1 Connexus complies with all relevant data protection and information rights legislation, including:

- UK GDPR
- Data Protection Act 2018 (DPA 2018)
- Data (Use and Access) Act (DUAA)
- Privacy and Electronic Communications Regulations (PECR)

14.2 We also consider guidance from the Information Commissioner's Office and meet the Regulator of Social Housing governance standards.

## 15. Monitoring and Review

15.1 Compliance with this policy is monitored through:

- audits and assurance activity
- reporting and learning from incidents
- review of data rights requests

14.2 Failure to comply with this policy may result in disciplinary action and, in serious cases, legal consequences.

## 16. Data Protection Officer

15.1 Connexus' Data Protection Officer can be contacted via email on connexus.GDPR@connexus-group.co.uk. The Governance team will monitor this email inbox if the DPO is unavailable for any reason.

15.2 Connexus' current Data Protection Officer is Nicola Topp, Information Governance Manager.

15.3 If the DPO is unavailable to assess and respond to any data protection issue then the Head of Governance and Risk and Company Secretary will act on behalf of the DPO and assume responsibility for the assessment, escalation and response to the issue, including any required regulatory engagement.

## 17. Appendices

Appendix 1 – Policy to Procedure Mapping Table

## 18. Document Control

| | |
|---|---|
| **Approved by ELT** | March 2026 |
| **Approved by Committee/Board** | 29 April 2026 |
| **Effective date** | 29 April 2026 |
| **Review date** | 30 April 2029 |
| **Policy developed by** | Information Governance Manager and DPO |
| **Consultations** | N/A |
| **Associated documents** | Procedures listed in Appendix 1 |

| Version | Author | Date Published | Next Review | Comments |
|---|---|---|---|---|
| 1.0 | Governance and Data Protection Manager | 25 Jul 24 | 31 Jul 27 | First version of the policy. |
| 2.0 | Information Governance Manager (DPO) | 11 May 26 | 30 Apr 29 | Policy updated to ensure compliance with current legislation including UK GDPR, DPA 2018, DUAA and PECR. |

## Appendix 1

### Policy to Procedure Mapping Table

| Policy Section | Policy Requirement (What the policy says) | Supporting Procedure / Document | Purpose of the Procedure | Owner |
|---|---|---|---|---|
| **1. Purpose** | Sets Connexus' high-level approach to lawful, fair and transparent data use | Data Protection Policy | Establishes organisational commitment and legal compliance | Head of Governance and Risk and Company Secretary |
| **2. Scope** | Applies to colleagues, board members, contractors and partners | Third Party & Contractor Management Procedures | Ensures third parties understand and comply with data protection duties | Head of Finance |
| **4. Data Protection Principles** | Personal data must be lawful, fair, accurate, secure and limited | Lawful Basis Guidance | Helps colleagues identify and document the correct lawful basis | Head of Governance and Risk and Company Secretary |
| **5. Roles & Responsibilities** | All colleagues must handle data safely and follow procedures | Mandatory Data Protection Training | Ensures awareness of responsibilities and good practice | Head of People |
| | DPO provides oversight and advice | DPO Operating Framework | Defines DPO independence, advice and escalation routes | Head of Governance and Risk and Company Secretary |
| **6. Collecting & Using Data** | Data must only be collected for clear, lawful purposes | Privacy Notice Framework | Ensures transparent communication with tenants, customers and staff | Head of Governance and Risk and Company Secretary |
| | Lawful bases must be identified | Lawful Basis Guidance | Prevents unlawful or excessive processing | Head of Governance and Risk and Company Secretary |
| **7. Sharing Data** | Data sharing must be lawful, necessary and proportionate | Data Sharing Procedure | Controls routine and exceptional data sharing | Head of Governance and Risk and Company Secretary |
| | Agreements required with third parties | Data Sharing Agreements & DPIA Guidance | Ensures safeguards are in place before sharing data | Head of Governance and Risk and Company Secretary |
| **8. Data Security** | Appropriate technical and organisational measures required | Information and Security Policy | Sets minimum security controls | Director of IT, Data and PMO |
| | Secure remote and flexible working | Hybrid Working Policy and Procedure | Protects data outside Connexus premises | Head of HR |
| | Safe handling of information | Information Classification & Handling Guidance | Helps colleagues apply appropriate controls | Director of IT, Data and PMO |

| Policy Section | Policy Requirement (What the policy says) | Supporting Procedure / Document | Purpose of the Procedure | Owner |
|---|---|---|---|---|
| **9. Data Breaches** | All suspected or actual breaches must be reported immediately | Data Protection Breach Procedure | Ensures rapid containment, assessment and ICO reporting | Head of Governance and Risk and Company Secretary |
| **10. Retention & Disposal** | Data must only be kept as long as necessary | Data & Document Retention Schedule | Defines retention periods and lawful disposal | Head of Governance and Risk and Company Secretary |
| | Secure disposal required | Records Disposal Procedure | Prevents unauthorised access after end of use | Head of Governance and Risk and Company Secretary |
| **11. Individual Rights** | Individuals can exercise their statutory data protection rights | Data Subject Rights Request Procedure | Ensures rights are handled lawfully and on time | Head of Governance and Risk and Company Secretary |
| | Connexus ensures that data protection complaints are taken seriously, investigated properly and responded to within legal timescales. | Data Protection Complaints Procedure | Ensures complaints are handled lawfully, fairly and escalated where required | Head of Governance and Risk and Company Secretary |
| **12. Transparency** | Clear information must be provided about data use | Privacy Notices (Tenants, Colleagues, Customers) | Meets transparency obligations under UK GDPR | Head of Governance and Risk and Company Secretary |
| | Connexus uses personal data for marketing and communications responsibly, ensuring people are not contacted inappropriately and that their preferences are respected. | Marketing & Communications Procedure | Ensures PECR compliance for electronic communications | Head of Communications and Marketing |
| **13. Legal & Regulatory Compliance** | Must comply with UK GDPR, DPA 2018, DUAA and regulator standards | ICO Guidance Monitoring Process | Ensures policies reflect current regulatory expectations | Head of Governance and Risk and Company Secretary |
| **14. Monitoring & Review** | Compliance must be monitored and reviewed | Internal Audit & Assurance Programme | Provides independent assurance of compliance | Head of Governance and Risk and Company Secretary |
| | Non-compliance may result in disciplinary action | Disciplinary Policy | Supports enforcement of policy requirements | Head of HR |