Data Protection Policy

Approved by	Audit and Risk Committee
Effective date	July 2020
Review date	September 2021
Policy developed by	Data Protection Officer / Head of Governance and Company Secretary
Associated procedure	Various – see policy text

Introduction

1. Purpose and Scope

1.1 **Purpose:** The purpose of this policy is to set out how Connexus will protect the rights of individuals regarding privacy and their personal data which is held by Connexus. It aims to ensure that all colleagues and board members are aware of their duties in relation to data protection and that there is a consistent, fair, proportionate and transparent approach to dealing with personal data across Connexus which is in line with legal and regulatory requirements.

1.2 **Scope:** The policy applies to the whole of the Group. This means Connexus Housing Limited, (ultimate parent) and all of its subsidiaries.

2. Introduction

2.1 Connexus holds personal and confidential information about tenants, former tenants, housing support service users, other service users, potential purchasers of our homes for sale, board members, employment applicants, employees and former employees, housing applicants and suppliers.

2.2 There are safeguards in data protection legislation and related regulations (including the General Data Protection Regulation) to ensure that such information – whether held on paper, in a computer, or recorded on other material - is collected and dealt with appropriately and proportionately.

2.3 Connexus is bound by data protection legislation (Data Protection Act 2018 – this incorporates GDPR into UK law) and related regulations and will ensure that the collection and storage of personal data, its processing and accessibility to it is carried out in line with the law and good practice.

2.4 Data protection is a responsibility shared by all colleagues of Connexus. Details of responsibilities regarding different aspects of data protection are set out in sections 3-13 below.

2.5 Connexus will ensure that colleagues, who are required to process personal data as part of their job, will receive training and/or guidance on data protection to ensure that all personal data is processed fairly and lawfully.

2.6 Connexus will take all reasonable steps to ensure that any organisation with whom we share data to enable it to carry out work on our behalf or for other legitimate purposes has robust and appropriate arrangements in place to ensure that personal data is handled lawfully and is kept secure.

3. Definitions

3.1 The following definitions are used in this policy: -

Data Subject – The individual whose personal information is being held or processed. A data subject is described as "any living individual person 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".

Personal Information/Data – Information about living 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, employees or board members of Connexus.

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:

- Race;
- Ethnic origin;
- Politics;
- Religion;
- Trade union membership;
- Genetics;
- Biometrics (where used for ID purposes);
- Health;
- Sex life; and
- Sexual orientation.

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

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 Housing 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 GDPR. For most purposes Connexus is the Data Controller, however there may be circumstances where Connexus acts as the processor.

Data Processor – Is defined as any person, company or other body (other than an employee of the data controller) who processes the data on behalf of the data controller.

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

Lawful Basis – The basis (as listed in the General Data Protection Regulations) 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 Data Protection Act 2018 and on which guidance is provided by the ICO.]

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

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

4. Overall Approach and General Principles

4.1 Connexus, including all colleagues and board and committee members will implement and comply with the six principles set out in the Data Protection Act 2018 i.e.:

- Personal data shall be **processed lawfully, fairly and in a transparent manner**;

- Personal data shall be **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- Personal data shall **be adequate, relevant and limited to what is necessary in relation to the purposes** for which it is processed;

- Personal data shall be **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

- Personal data shall be **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed**; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Act 2018 in order to safeguard the rights and freedoms of individuals;

- Personal data shall be **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage**, using appropriate technical or organisational measures.

5. Obtaining Data

5.1 When Connexus collects personal information from a data subject for the first time and when any new data is collected. Connexus will disclose and explain: -

- why the personal information is required and held on record;
- the purposes for which the data may be used; and
- who may have access to the data.

5.2 Connexus will ensure that the 'lawful basis' for collecting and processing personal information is identified and recorded.

5.3 Where consent for processing personal information is obtained, Connexus will ensure that the options are clear, that consent is freely given and clearly recorded. We will take reasonable steps to ensure that the data subject understands why they consented to provide the information and the consequences of deciding not to give this consent.

It should be noted that where consent has been given the data subject has the right to withdraw this consent at any time. Where consent is withdrawn this should not impact on the service provided.

5.4 Where we collect and hold more sensitive personal data (including that described by the law as 'special category' information) we will always seek clear consent for this, explain why we need it and who we may need to share it with. We aim to minimise the holding and use of this type of personal information but given the service we provide there are times when we use it e.g. when providing accommodation or support for someone who has disabilities or problems with substance abuse, when helping someone to access care services or when resolving neighbourhood disputes. We use stricter limits for access to this information within Connexus.

5.5 Connexus will take reasonable steps to ensure that personal data is kept up to date and to encourage data subjects to notify us of changes but cannot be held responsible for any errors or inaccuracies in personal data being held and processed where the data subject has not provided updated information or told Connexus that the data it holds is incorrect.

6. Security of Personal Data

6.1 Connexus is committed to ensuring that personal data remains secure whatever format it is stored in. Connexus recognises individuals' rights to privacy and their expectation that all personal data held about them will be handled sensitively and in accordance with the law.

6.2 Connexus takes appropriate steps to keep its ICT systems secure to protect personal data from unauthorised access, disclosure and/or loss. These measures will include:

- Use of passwords
- Anti-virus and anti-malware/ransomware software
- Firewalls
- Email and web filters
- Application of software updates/patches
- Use of secure transfer arrangements (e.g. secure email or encryption)
- Role based access rights to systems holding personal data.

6.3 Personal data must be kept secure at all times. All colleagues must ensure that they take appropriate measures to keep personal data and/or confidential information secure by, for example, keeping passwords confidential; changing passwords regularly; filing information appropriately; locking drawers and filing cabinets and so on.

6.4 Connexus will give colleagues and, where relevant, board members advice on the necessary physical security arrangements to be adopted appropriate to the level of confidentiality of the personal data concerned. Connexus will also provide guidance and/or procedures on keeping data secure such as: -

- when personal data is taken out of the normal place of work;
- backing up data securely;
- destroying data securely;
- when communicating with individuals, ensuring the authenticity of that individual before the personal data is processed (or disclosed); and
- restricting access appropriately to manual and electronic files and ensuring necessary steps are taken to ensure security of data when it is being processed.

6.5 Where other organisations are contracted to carry out work on our behalf, Connexus will set out clear expectations regarding the contractor's role in the protection of personal data (such as tenant contact details provided to repairs and maintenance contractors).

6.6 Colleagues and customers will be offered a private place to discuss personal and/or confidential information.

6.7 It is the responsibility of all colleagues to report any data security breaches and suspected breaches, relating to unauthorised access to or disclosure of personal data. Such incidents should be reported to the Company Secretary without delay. Colleagues should refer to and follow the data breach procedure when such incidents occur.

6.8 We will take all reasonable steps to ensure that any organisation with whom we share data notifies Connexus of any data breach, where this relates to or may relate to personal data which we have shared with them.

6.9 All data breaches will be investigated, and lessons learnt will be circulated widely to minimise the chances of a future breach.

6.10 Data breaches may be reported to the Information Commissioners Office (ICO) if, in the opinion of the Data Protection Officer (DPO) or Head of Governance and Company Secretary or Member of the Executive Management Team (EMT), there is a requirement to do so in line with ICO data breach guidance.

7. Security of Personal Data

7.1 In order for Connexus to operate effectively there will be some instances when personal data will need to be disclosed and/or discussed with other appropriate individuals. In such instances this disclosure, whether it is written or verbal, must be appropriate and reasonable for business purposes, on a need to know basis only and in line with data protection legislation and, where possible, in accordance with ICO guidance.

7.2 Colleagues will not attempt to gain access to personal data that is not necessary for them to hold or relevant for them to carry out their normal work.

7.3 Connexus may enter into information sharing protocols with other organisations. These enable Connexus to deliver some of its services more effectively and can also help reduce the amount of times individuals have to disclose the same personal information.

7.4 All data sharing protocols must be agreed by the DPO or, in the absence of the DPO, the Head of Governance and Company Secretary, recorded centrally and reviewed periodically to ensure that they are still appropriate.

7.5 Personal data relating to individuals will be considered confidential and will only be passed to other organisations with the express written consent of the individual concerned unless they are directly related to our responsibilities and legitimate interests as a landlord (such as basic tenant contact details provided to enable a contractor to carry out repairs or improvement works or to obtain customer views on our services) or where there are exceptional circumstances (see paragraph 7.6 below). In most cases, Connexus will seek initial consent from data subjects to process data and will explain why and to whom that data may be disclosed.

For example to comply with Connexus' legal obligation to provide information to the Department for Works and Pensions and HMRC.

7.6 In exceptional circumstances, Connexus may disclose information to authorised third parties without the data subject's consent. Such circumstances include: -

- where there is clear evidence of fraud;
- to comply with the law;
- in connection with legal proceedings;
- where it is essential to enable Connexus to carry out its duties;
- where the health and safety of an individual would be at risk by not disclosing the information; and
- where the data is anonymised and to be used for statistics/research.

7.7 Requests from third parties for such access to personal data will generally only be considered where these are made in writing, when Connexus is satisfied as to the purpose for the disclosure and, where applicable, is in accordance with the relevant information sharing protocol.

7.8 Connexus will not disclose any personal data either verbally, or in writing, to any unauthorised third parties.

7.9 Connexus will never disclose data to those who are not otherwise authorised to process it without a data subject's prior consent.

7.10 Details of Connexus' 'Privacy and Cookies' statement are available on our website at https://connexus-group.co.uk/privacy-cookies.

8. Retaining and Disposing of Data

8.1 All personal data that is held will be relevant for the purpose for which it is required and will be kept securely. It will be retained for periods laid out in Connexus data and document retention schedule (a copy of which is on the intranet) and for no longer except where a contract requires otherwise.

8.2 Some personal data is held and processed by Connexus in order for us to provide services under a contract for another organisation (such as housing support contracts for a local authority). In these cases, we may be required to retain personal data for the duration of the contract or for a set period beyond the end of the contract.

8.3 Where personal data is no longer required, it will be destroyed in a secure manner or in the case of a contract carried out by Connexus, if required, returned to the organisation which commissioned the contract.

9. Access to information

9.1 Individuals (data subjects) may request a copy of information held about them by Connexus (a Data Subject Access request) and can seek to have it amended or erased if it is inaccurate or no longer required (the 'right to rectification' and the 'right to erasure').

9.2 Connexus will respond to any subject access requests as quickly as possible, but within the required period i.e. within 30 calendar days of receipt of the request. Where it is not possible to complete a request the data subject will be informed in writing, with a full explanation. In circumstances where there may be a delay in completing a request, the data subject will be informed with a full explanation.

9.3 When a request is made, Connexus must be completely satisfied the applicant has the authority to request such information. If Connexus has any doubts as to the authority of, or the identity of any applicant, a request may be refused. A request may also be refused if part of the data relates to another individual who has reasonably refused to their personal data being disclosed, a similar request was recently complied with, or the request would require a 'disproportionate effort'.

9.4 Individuals have the right to receive a copy of information held about them by Connexus free of charge. Connexus reserves the right to make a reasonable charge for responding to requests which are excessive or repetitive.

9.5 See data subject access request procedure for more details.

10. Other Rights

10.1 Connexus will put in place appropriate arrangements to enable an individual to exercise their other rights under the DPA 2018.

10.2 The Act provides the following rights for individuals:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making and profiling.

11. Information about Data Protection

11.1 Connexus will publicise its approach to data protection, including information about:

- What data the organisation holds and processes and why;
- How to gain access to personal data;
- How personal data is kept up to date;
- How personal data is kept secure;
- What Connexus is doing to comply with its obligations under the law.

11.2 Such information will be made available on our website(s) and, where appropriate, in our offices and/or communal rooms used by tenants and/or service users.

12. Legal and Regulatory Requirements

12.1 Connexus will comply with all data protection legislation including the Data Protection Act 2018.

12.2 Connexus will also comply with relevant regulatory requirements regarding data protection. The Regulator of Social Housing's standard on governance and financial viability includes the requirement for Registered Providers to "ensure effective governance arrangements that deliver their aims, objectives and intended outcomes for tenants and potential tenants in an effective, transparent and accountable manner"; this includes adhering to all relevant law and complying with all regulatory requirements.

12.3 Where Connexus or parts of Connexus are affected by Charity Commission (CC), we will abide by any such requirements. We will also take any good practice in probity published by such bodies into account when formulating Group wide policies and procedures.

12.4 Connexus will consider guidance from the Information Commissioners Office when devising policies, procedures and practices related to data protection.

13. Responsibilities

13.1 Data protection is a responsibility shared by all Connexus colleagues.

13.2 Each Director is responsible for the implementation of this policy in their area of responsibility and for ensuring that colleagues receive appropriate briefing on the specific data storage, processing and disposal requirements of their post in accordance with this policy and associated Connexus procedures and guidance.

13.3 Each Director is responsible for ensuring that any contractors with whom they share personal data (e.g. in connection with the provision of services on behalf of Connexus), are advised of any requirements relating to the use, storage and destruction of such data.

13.4 The Head of HR is responsible for ensuring that all newly appointed colleagues are advised of the basic requirements regarding data protection – including the information set out in the employment contract and that relating to their own personal data – in their initial induction.

13.5 Line managers are responsible for ensuring that newly appointed colleagues or colleagues taking up different roles within Connexus are advised of data protection issues and guidance specifically relevant to their role.

13.6 All Connexus colleagues are responsible for familiarising themselves with this policy and with Connexus's rules, procedures and guidance relating to data protection, and must follow these at all times.

13.7 Connexus colleagues are responsible for ensuring that all personal data they process/handle is kept as up to date and accurate as possible and that any changes to personal data, notified by the data subject are acted on promptly.

13.8 All Connexus colleagues are responsible for ensuring that all personal data they process is kept secure.

13.9 Connexus colleagues are responsible for ensuring that all personal data they provide about themselves (e.g. to the Human Resource team for employment related purposes) is accurate and updated when appropriate.

13.10 All Connexus colleagues are responsible for informing the DPO or, in the absence of the DPO, the Head of Governance and Company Secretary of any data protection breach and for following the data breach procedure.

13.11 The DPO or, in the absence of the DPO, the Head of Governance and Company Secretary is responsible for notifications of any data breach to the Information Commissioners Office.

13.12 The DPO or, in the absence of the DPO, the Head of Governance and Company Secretary is responsible for review of this policy and for ensuring the production of associated guidance.

13.13 The DPO or, in the absence of the DPO, the Head of Governance and Company Secretary is responsible for maintaining appropriate registrations with the Information Commissioners Office.

14. Monitoring and reporting

14.1 Connexus will monitor implementation of the policy through annual reviews and internal audits.

14.2 Connexus will record data access requests and monitor responses to such requests.

14.3 Failure to comply with this policy may lead to disciplinary action and depending on the nature of the breach may lead to summary dismissal. Breach of this policy may also constitute a criminal offence.

15. Review

15.1 Connexus will review this policy at least every 3 years and these regular reviews of the policy take account of any changes in regulatory guidance and good practice. A review will be carried out sooner should there be any changes to legal or regulatory requirements.

16. Data Protection Officer

16.1 Connexus' Data Protection Officer can be contacted via email on connexus.GDPR@connexus-group.co.uk.

17. Statement

In relation to the requirements of Article 38 of DPA 2018, Connexus is committed: -

17.1 The controller and the processor (being Connexus Housing Limited and all its subsidiaries) shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

17.2 The organisation shall support the DPO in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

17.3 The Organisation shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks. The DPO will not be dismissed or penalised by the Organisation for performing data protection tasks. The DPO shall directly report to the highest management level of the Organisation

17.4 Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

17.5 The DPO shall be bound by secrecy or confidentiality concerning the performance of data protection tasks, in accordance with the DPA 2018.

17.6 The DPO may fulfil other tasks and duties. The Organisation shall ensure that any such tasks and duties do not result in a conflict of interests.